A systems-based approach to integrating security risk management into the management practice & culture of a global multi-national organisation

A project submitted to MIDDLESEX UNIVERSITY in partial fulfilment
of the requirements for the degree of
Doctorate of Professional Studies

Jeremy Christopher HART
BA (Hons) MSc

Candidate No: **M00388432**

July 2018

INSTITUTE FOR WORK BASED LEARNING

ACKNOWLEDGEMENTS

I would like to extend profound thanks to my Middlesex University adviser, Professor Paul Gibbs, for his advice and guidance throughout my studies, and to my technical advisor Dr Jyoti Navare.

My studies were funded by my company for which I am extremely grateful and I look forward to honouring its investment for many years. I owe a profound debt of gratitude to my Line Manager and General Counsel, Dr Olivier Merkt for agreeing to finance my research and supporting me in gaining the necessary access to conduct my field work. I also wish to thank for their support the initial Project Sponsor and former Senior Vice President for Strategic Transformation, Mr François Marti and Vice President for Strategic Transformation, Mr Filippo Rota.

I am extremely grateful for the invaluable comments and support of my colleagues at Corporate Security and the managers and other employees in all the countries that facilitated my fieldwork. I also owe a significant debt of gratitude to past colleagues at the University of Leicester, particularly Professor Martin Gill, Professor Adrian Beck and the late Professor John Benyon, for helping me start my journey in security risk management.

Finally, I would like to thank Mr Gareth Evans, former Resident Twinning Adviser to the Government of Kosovo and Counter-Terrorism Liaison Office at the DVLA for his invaluable technical insights on document falsification, which helped sow the earliest seeds for this project, and to Mr Andrew Fisher, formerly of the Royal Air Force Police, who facilitated my first opportunity to apply academic learning to workplace practice.

As with all my work, this project is dedicated to the security and happiness of my wife and family and in thanks for their ongoing and patient support.

Disclaimer: The views expressed in this document are mine alone and are not necessarily the views of my supervisory team, examiners, Middlesex University, my company or its employees.

CONTENTS

ABSTRACT

I work in the Corporate Security department of a global multi-national company that operates a wide range of businesses in many complex and turbulent environments, including developing countries and those recovering from conflict or similar strife. To help deliver the best level of protection for people, assets and business processes, my project sought to find an innovative, cost-effective and non-disruptive approach to integrating security risk management into the mainstream management practice and culture of my organisation. The solution needed to be responsive both to global corporate policy, the ontological and epistemological stances of the diverse professions within the company and the demands of the security risk environments where we conduct our business.

The project's theoretical framework is inherently multi-disciplinary and derives from theories of crime and theories of risk and the fusion of these with theories of management and organisation – particularly those related to systems theory. It provides a powerful platform for an innovative approach to security risk management to help to locate it alongside other key disciplines within the mainstream requirements for management thinking, knowledge and ability.

I developed the approach while conducting internal security risk assessments and corporate security investigations, and while contributing to my company's consultancy work for external organisations. The project is reflexive in that it has required me to reflect on, evaluate and enhance ways of working that I have acquired by experience and various forms of learning, alongside the various theoretical models that I refer to.

I gathered the project data using focus groups, interviews and participant observations, and incorporated elements of *bricolage* into my methodology to cope with unpredictable field conditions and other disruptions, which were numerous. My project's analytical framework is based on a *sensemaking* approach, derived from the project's theoretical framework. The units of analysis are case studies of my treatment of businesses in a range of different industries and countries. In addition to evaluating the security implications of explicit formal structures, such as physical design or documented procedures, it also emphasised the significance of 'soft' inputs, such as employee perceptions of risk and various styles of management. Collaboration with technical experts enabled mutual learning and significant steps towards designing-in security to systems and processes.

The project's success was to be defined by the endorsement of the senior corporate and local managers who are ultimately responsible for risk management. It has achieved this goal, manifested in recommendations to use the approach to address a wide range of business challenges. This is supported by testimonials to the effectiveness of the approach and a growing commitment to embedding it within the company's businesses via training and education programmes which I am currently developing.

My conclusion summarises the project and argues that security risk management is about changing and managing perceptions of opportunities to offend. These include the perceptions of managers and others who support the organisation's objectives and goals, as well as those of potential offenders who would otherwise perceive organisational assets and processes as attractive targets.

TESTIMONIALS

Please note that these testimonials were presented in full for the information of the Examiners but have been redacted in this edition for reasons of confidentiality.

CHAPTER 1: INTRODUCTION

About my project

My project is about security risk management, a management discipline and organisational function that integrates assessment of the risks of intentional harm with the implementation of strategies, tactics and techniques to protect people, property and functionality.

As a management discipline, security risk management is inherently multidisciplinary and derives from various forms of knowledge about *security* and the actions and behaviours that threaten it; about *risk* and how to identify, assess and respond to it; and about *management* – the body of knowledge concerned with the nature and characteristics of organisations and their structures, activities, processes and culture.

My project explores the contribution of these subject areas and the epistemologies that underpin them by reviewing the relevant literature and reflecting on my own practice and positionality as a security risk manager. It presents my approach to security risk management as an innovative, business-oriented and transferable collection of tools, techniques and knowledge-bases. I've named my approach 'Business Process Security Analysis' (BPSA) because it visualises businesses as *systems* that are amenable to analysis and identifies and assesses security risks at the *process* level.

As an organisational function, responsibility for security risk management in most organisations rests within a specialist corporate security department. These typically apply the existing and accepted approaches and standards for assessing and managing security risks, which I will review in due course. However, when I tried to implement them in my organisation, I was dissatisfied with the process they involved and unconvinced by the results they produced. This was because they require data that is often either unavailable, unreliable or out of date and are designed for use by 'risk experts' rather than managers with no specialist security risk management training. In my organisation and most others, security risk experts are embedded in parts of the organisational structure that are far removed from the processes and locations where security risks emerge. Those who are closest to the action are not considered experts in security risks – and they rarely benefit from any associated education or training. Consequently, security risk management is not sufficiently incorporated into the business configuration, which leaves the risks untreated and the business and its assets exposed – until an incident occurs.

Even where risk assessments have been conducted, their focus tends to be too 'high level' to have the kind of impact that my approach achieves. Wakefield (2014) addresses this, citing an empirical study by Speight:

> A recent doctoral study by Speight (2012), based on research carried out in 2006 to 2009, identified that almost all the organizations surveyed had implemented security measures that addressed only generic risk, rather than specific risks identified through appropriate security risk assessments. This suggests that there is substantial room for improvement in typical corporate security practice.
>
> Wakefield, 2014: 251

I believe that a lack of knowledge and awareness of security risk management among managers who are not specialists in this discipline limits the effectiveness of the most prevalent structural model for security provision. I believe that some level of security risk knowledge should be integral

to generic management competence, and should appear in the future curricula of management training courses and in the list of required skills for manager recruitment. BPSA to some extent addresses this gap for those already in post with a collaborative approach to data gathering that involves security specialists and business process specialists working together and sharing their knowledge. As Haimes (2015, citing Covey) notes:

> Unlike previous processes where a design group would throw plans *over the wall* to manufacturing, representatives from manufacturing are included in the design process from the start. The importance of developing a shared understanding from both perspectives is obvious.
>
> Haimes, 2015: 12

In the analytical phase of my approach, collaborative teams apply their various disciplines to understand situational, motivational, perceptual and other factors that provide insights about how to formulate preventive and remedial action that support business functionality and goals. This process of sensemaking generates individual and group experiences that can be shared with a wider audience. I believe these and other project benefits to provide a practical, transferable workplace-based means of working towards the ambitious goal of integrating security risk management into mainstream management practice and culture.

I developed and tested my approach while conducting security risk management assignments for my company in many different countries and business sectors around the world. The next section provides an overview of this complex project setting.

Project setting

Security risk management is an omnipresent activity that protects people, activities and property in all sectors in public, private and virtual space. My company operates in all of these, but in the specific context of a private sector global multi-national commercial organisation. Although it must be understood in this context, I also believe that the approach I developed is applicable to other types of organisation or enterprise, including government and not-for-profit entities.

My company provides inspection, testing and certification services to a diverse range of market segments, including agriculture, hotels and hospitality, manufacturing and retail, minerals, oil, gas and chemicals, pharmaceuticals, and sea, air and land transportation. It also provides various forms of support to governments, such as assisting with border inspections, facilitating customs and excise activities, forestry management and much more. Headquartered in Europe, this large and complex international trade facilitation organisation employs 95,000 people at over 1,500 sites located in around 150 countries worldwide.

I conducted the project research in my role as Global Security Risk Manager within the Corporate Security department. My department provides security advice on request to all my company's businesses in all the territories where we operate, and conducts security risk assessments and integrity investigations on behalf of the global Legal and Compliance function to which it is accountable. The department is small, comprising solely two field-based (including myself) and two office-based operatives. All are resident in the United Kingdom, but field operations can take place anywhere in the world. We also have a network of local representatives in various countries, but they have full-time roles in other functions and primarily serve as conduits for gathering and reporting information. These structural features of my department are relevant to my project,

because our obvious capacity limitations have important implications for the responsibilities of non-security specialist managers in our businesses and territories.

Business operations in each country are managed by wholly-owned subsidiaries, which the global company refers to as *Affiliates*. The relationship between the Affiliates and the global 'Group' management presents the latter with some significant challenges to maintaining consistent yet adaptive systems and culture. Although bound by many centralised policies and standards, Affiliates may have become part of the company by acquisition, thereby bringing a legacy culture that needs to be 'on-boarded'. They also have a high degree of autonomy to allow them the flexibility to adapt to local business conditions, which include the demands of the local security risk environment. This has specific implications for the types of knowledge and expertise they need access to and the corresponding levels of detail that should be available to the security function about business activities.

Security knowledge and the security function

This section discusses the epistemologies that contribute to the security function and its partial isolation within many organisations.

As mentioned in my opening paragraph, security risk management is a complex and inherently multi-disciplinary subject that arguably 'lacks definition and structured knowledge' (Brooks and Corkill, 2014: 219) when compared to other management disciplines. However, there is some consensus that its ontological and epistemological foundations are found in applied criminology, risk theory and management studies. These derive from a range of other disciplines, including social and natural sciences, as well as law and even medicine. There is also a technical side to security and security technology that is more closely related to engineering and physical sciences, although this aspect is not the primary focus of my project.

Security knowledge is acquired by a combination of practical experience and technical and academic research and teaching. In terms of experience, there is a tradition of practitioners having a law enforcement or military background. This is highly respected within the practitioner community and in the relatively recent past was an expected 'qualification' for a security career. However, sources within the recruitment sector have noted that many employers no longer share this view – possibly indicating a changing expectation of what they expect the security function to contribute to organisations:

> … clients are increasingly requesting candidates who have not had a long first career in the police or armed forces because they want to avoid candidates encumbered by the kind of experience that encourages a 'boxed' way of thinking about security.
>
> Briggs and Edwards, 2006: 82

This 'boxed way of thinking' deserves more exploration than the scope of this report allows. However, it refers to certain dogmas and inflexibilities that security practitioners may bring from their earlier careers and that are not perceived as sufficiently supportive of business goals and objectives. As one chief security officer writing in CSO magazine noted about former law enforcement officers:

> ... the corporate security field can be worlds apart from their experience working in law enforcement … I need them to have skills they do not possess; I need them to have a viewpoint they do not understand (and often resist); and I need them to do things they do not like to do.
>
> Anonymous, 2005: 52

There are therefore differing views on the type of knowledge that security practice requires, depending on the context of its application. Some businesses – particularly in the high technology sector, but also in banking, mining and petrochemicals – place a great deal of emphasis on technical solutions to security challenges, so knowledge of computer networks, alarm systems, access control, video surveillance and advanced barrier technologies is highly prized. Meanwhile the security needs of other organisations may demand more insight into human behaviour or the security and integrity of business processes. In my organisation, I am more closely aligned with the latter orientation, while a close colleague specialises more in technical security matters.

Technical competence in security is facilitated by the many professional and trade associations offering training and vocational qualifications in various aspects of security practice. This is a trend that started in the 1970s to remedy the lack of recognised and trusted professional credentials in security (Walby, Luscombe and Lippert, 2014: 123). However, it wasn't until the late 1980s when security risk management started to attract more academic attention and began to appear in higher education programmes. It is now studied as a specialist subject up to and beyond postgraduate level in various universities around the world. Providing further evidence of the diversity of perspectives on security learning and research, institutions locate the subject in a range of different faculties depending on their specific epistemological view. These include social sciences (University of Leicester), law (University of Portsmouth), and engineering (Edith Cowan University, Australia) as just some examples.

Combining experience with technical training and academic knowledge is part of a conscious effort to present security as a new profession that is represented by professional associations, discussed and explored in professional and scholarly journals and respected by professionals of other disciplines. However, it is curious that research on this emerging profession indicates that the level of subject-specific knowledge required 'will decrease as the security manager moves from front-line to executive management' (Brooks and Corkill, 2014: 223). This is in marked contrast to the other, more established professions that are also found in organisations, such as law. There is a sense that the security manager is:

> … a hybrid agent, neither fully situated within the field of security nor in the field of business but constantly trying to negotiate the meaning of difference.
>
> Petersen, 2014: 83

Security practitioners who seek promotion must therefore acquire generic business knowledge. So, while subject-specific higher education programmes in security risk management remain popular, the need for practitioners to present themselves as 'business-oriented' influences some to pursue their professional development through generic management programmes, such as MBA courses. However, thinking in terms of reciprocity, these rarely include security as a subject in their curricula, so management students who do not have security experience are not exposed to the subject in the lecture theatre.

Rather than raise the profile of security as an integral aspect of management and a new opportunity to achieve excellence, these arrangements would seem to brush the discipline into the side lines and away from the core management activities of planning, leading, organising and controlling the organisation (Fayol, 1916). This is further exacerbated by an organisational tendency to isolate security experts from other organisational functions, which is sometimes justified with reference to the security department's 'policing role'. When I first started to study security, it was common to hear experienced 'old guard' practitioners refer to the historic definition of the 'Provost' or military police as 'but one man [who] must correct many and therefore he cannot be beloved' (RHQ RMP, 2018) – i.e. the security function must not allow anyone to get too close. Another reason might be a perception that security is an add-on – an option to be considered when needed, but not before, or even as a negative function and an obstacle to business development – until something happens:

> … security is always too much when nothing happens and never enough when an incident occurs.
>
> Rovers, 2014: 1

It is also possible that there is an emerging distinction between the technical *administration* of security *measures*, such as the management of guards, technologies and associated out-sourcing contracts, and the identification and diagnosis of security *risks* that are embedded in business processes.

In terms of the latter, which is the aspect that most concerns my project, it is difficult to nurture and maintain a centralised specialist capability that is possessed of sufficient intimate knowledge of all businesses and all territories to provide meaningful guidance and remain relevant. Further, attempting to manage security risks from the organisational centre risks pushing a bland, one-size-fits-all totalitarian approach that is insensitive to the different operating conditions, risk environments and assorted regional and professional cultures within the organisation.

Some organisations tackle this by distributing their security experts across the entire area of their operations. However, this is expensive and they can still remain isolated in the way just described even at the local level. The security function can also be subsumed within the local power structure and fall under the influence of parochial management at the expense of safeguarding the universal values that the organisation seeks to establish and maintain.

In my company, responsibility for the administration of security is delegated to the most senior employee (designated Country Manager or Managing Director) in each country. In principle, this delegation is sensible because it requires security to be combined with the other adaptive strategies which Country Managers must apply. However, we are left with the problem of a knowledge deficit, as these individuals are not security specialists and the company does not require them to complete any security training or even to consult with security specialists. Neither does it require them to submit any security plans or policies. In the case of my company, my department does publish generic security guidance, but this documentation does not address the subject in a sufficiently intimate way to achieve the best possible fit with the wide range of business and local contexts in which it needs to be applied.

The resulting configuration places the dedicated security department in a reactive 'policing' posture to be called upon *after* incidents occur. When they do, security specialists are deployed to

investigate what happened, find out who is responsible and – if the perpetrator was an insider – to gather evidence for disciplinary action, such as termination of employment. Although they may accept some advice about implementing an engineering solution, such as adding a few CCTV cameras or building a taller fence, local management may then consider the matter closed. Yet this is a lost opportunity to identify the systemic failures that allowed the incident to happen, and to make the systemic changes that are necessary for future prevention.

The reactive policing model of the security function is in marked contrast to that found in the relatively new information and communications technology sector, where 'usability, performance, reliability, *and security* indicates the success of the design and the overall quality' (Microsoft Corporation, 2009: Ch 16, emphasis added). Writing of Crosby's 'zero defects' approach, Kathawala explains how the concept of prevention and learning from mistakes are fundamental to achieving quality:

> The system used to obtain quality should be one of prevention, as opposed to one of appraisal. This means that a problem must be identified before it occurs rather than after, so that it can be remedied. Crosby goes on to say that mistakes are not a built-in part of humans, but are a result of the lack of importance that people place on doing certain tasks. The other factor that contributes to human errors is the lack of knowledge which could be corrected through trial and error.
>
> Kathawala, 1989: 10

Protective and preventive security needs to be incorporated into the design of products and services from the outset and maintained throughout the value chain, rather than summoned as a fire-fighting afterthought when things have already gone wrong. Indeed, as Haimes (2015) notes, this applies to the wider risk management effort:

> Thus, risk assessment and management must be an integral part of the decision-making process, rather than a gratuitous add-on technical analysis.
>
> Haimes, 2015: 4

For these reasons, it is necessary for security risk management to enter the management mainstream, alongside recognised epistemologies such as finance, human resources, health and safety and legal with the goal of building a culture and practice of trust, as well as a means of managing it. The systems approach that forms the foundation of my project helps embed this trust deep within the business processes of the value chain.

How the project evolved

This was a two-stage project that started off with a much narrower scope than the offering presented in this final report. The first stage sought to explore how the security risk management function could help the company achieve a competitive edge by enhancing the quality of service and reassurance it affords its customers. The specific vehicle for this initiative was my company's issuance of certificates and reports. These are printed on specially manufactured paper and the certificates are recognised around the world as legal instruments that present and affirm the results and findings of its audit, inspection and testing work. Many governments will not allow goods to cross their borders unless such documentation accompanies them and they are also used to secure loans from banks and often feature in the conditions of contracts and trade agreements. They are, in many ways, a physical embodiment of the company's primary offering (*trust*) and are therefore attractive targets for falsification and other forms of attack, so I wanted to find a better

way of protecting their authenticity. Inspired by some previous work I participated in on the authentication of individual identity afforded by biometric passports, I wanted to find a way to inextricably link the commodity or service with the documentation that authenticated it.

The traditional approach to the security of such documents is to print them on special media, known as *security paper*. This is manufactured in Switzerland using many of the techniques involved in the production of currency and other sensitive documents and has many physical security features, including graphical overlays, special inks, inverted characters and other features that make it very difficult to counterfeit. Every sheet must be accounted for and stocks at each branch must be kept in secure conditions. There are also strict procedures about the dispatch and distribution of replenishment stocks that require all deliveries to be recorded and any losses to be reported and investigated. Sheets are individually numbered in sequence and these numbers are recorded whenever the sheets are either used, damaged or spoilt. Although hard copy documents are gradually being replaced in many countries and industries with a digital alternative, many governments, regulatory bodies and financial institutions still require a printed version presented on the traditional media.

The problem is that security paper is not very secure. My company was (and still is) experiencing a year-on-year increase in queries and complaints about the provenance of our certificates, which have proven vulnerable to falsification, alteration and misuse. This is sometimes done by third parties seeking to perpetrate a fraud or similarly criminal act, or by customers seeking to avoid paying the fees for a new service and fresh certificate. However, these are critical issues for those who rely on the documents – for example, when planning to use the commodities they refer to as food ingredients or safe building materials – as well as for my company's reputation for accuracy and integrity.

I therefore decided to use my doctoral research to evaluate the effectiveness of existing protective arrangements and countermeasures and to explore whether technical or procedural security enhancements might offer a cost-effective improvement. However, I needed to find a way of identifying and assessing the vulnerabilities and risks. By conceptualising the production and use of these documents as a system, I sought to map the processes to identify the vulnerable points using a systems-oriented approach that I had used in a more rudimentary form in previous projects. I then intended to implement change and to measure any difference in security performance – such as a reduction in the number or type of relevant incidents.

This was a tidy and finite project that resulted in a series of recommendations including a strategic change from paper-based to digital authentication systems. However, my findings took me to a point where I needed the company to commit to running a pilot project and allocate the necessary resources. This would have allowed me to compare 'before' and 'after' states to evaluate the effect of the change as I envisaged in my project proposal when I wrote:

> Although I cannot take responsibility for every phase of the proposed project implementation, I will play pivotal roles throughout, thereby affording me with the opportunity to evaluate and reflect on the impact of each phase on those that follow it.
>
> DPS4561: 8

At the time of writing, I am still waiting for this to be approved, but the company has other priorities. This was a major disappointment, to say the least, because it seemed to deny me the clearest way of demonstrating how my research could produce a positive and significant change.

However, my approach to analysing the authentication problem had generated a lot of useful findings about hidden and unknown risks and this had attracted positive attention within the company. It was perceived to reach deeper into how the businesses worked and where the vulnerabilities lie than traditional approaches which seek to surround them with layers of physical protection. Managers understand systems, so framing the security risk problem within a systems approach provides a format they can easily relate to and which helps them recognise its impact on overall performance.

I was therefore asked to apply my approach to other security risk issues that lay beyond my original project scope. This second stage of my project included evaluations of specific security technologies, security risk assessments of specific services or projects, formulation of risk reduction strategies in various businesses, and investigations of suspected criminality. The approach has so far proved both versatile, robust and readily applicable to any setting. Crucially, it generates findings, observations and solutions that all managers seem able to engage with and convert into positive action.

However, this second stage was to address a messy problem. Different business lines are exposed to different kinds of security risk, yet awareness of these is far from uniform among those who work in them and the preparedness of managers to engage on security issues varies considerable. The many different professional groups in my company have different and sometimes conflicting world-views and language is inconsistent between these groups, and even more so between different territories where ‘false friends’ translation problems and semantic nuances abound. Environmental variables such as social and political settings also vary so, for example, the degree to which private entities can rely on support from public security provision, such as the police, span the full range of positive to negative possibilities.

The second stage also forced me to find ways of thinking about and articulating some aspects of my own subject matter. One of the key issues I had to re-visit is the nature of risk, which I had hitherto accepted as ‘something measurable’ and separate from the view of risk that exists in the perceptions of individuals and groups. My views on this changed during the course of my project, as did my onto-epistemological stance and my understanding of what constitutes a successful outcome from applying the approach. The reality I had to confront was that previous attempts to measure security risks using the established approaches had made little impact on management decision-making in my organisation. What I needed to do – and what feedback from many managers reassures me that my approach has achieved – is to change managers’ perceptions of risk *as a problem* to persuade them to *engage with* attempts to manage it. BPSA achieves this because of its granularity and its analysis of security risks from multiple perspectives, including those of business process experts.

My methodology chapter explores this in more detail, but in essence I structured my project using case studies to allow each to be understood in its own enclosed context, while being able to

develop the approach for the next case. I resorted to a bricolage approach to many aspects, because the operational demands of my role were unpredictable and disruptive, so I had to improvise solutions to enable the project to continue. I also embraced a more phenomenological approach to better understand actor perceptions, especially on risk, but also on their working environments and the prevailing management style and culture.

In terms of defining a successful outcome, the most affirmative way would be to demonstrate a reduction in security incidents. The problem I sought to address during the first phase of the project was characterised by a sufficient volume of reported incidents to enable me to at least demonstrate a downward trend in the volume of incidence (if, indeed, I could have reasonably attributed such results to my intervention). However, this is not the case with the second stage, because some of the case studies addressed concerns that were not fuelled by security incidents, and those that were involved low frequency but higher impact events.

Project aims

As my project evolved, I decided it should try to achieve the following aims:

- *Quickly make sense of unfamiliar problems*
    - I needed a way of making sense of complex businesses and risk environments of which I had little knowledge or experience.
- *Create a positive impact*
    - I needed to offer solutions that enable and enhance the business process, rather than obstruct or hinder it.
- *Share the knowledge and the experience*
    - I needed my approach to be accessible to people with no security risk management training and to generate new knowledge to be shared with others

I will revisit these aims in Chapter 7 where I present my findings.

Project impact

The project has received very positive feedback from managers at strategic, tactical and operational levels. At the leadership level, my line manager is particularly pleased with the engagement my approach has enabled with business managers and other employees at all levels. This is because it has brought the security risk management function much closer to the business and provided evidence of its potential to make a positive impact. For me, the most significant remarks from these groups are those indicating a change in approach to project planning and execution (e.g. in new contracts), as this is the point when security risks should be considered, rather than later when something goes wrong.

I am also pleased to have been invited to apply the approach to outward-facing commercial projects for external customers. These involve billable projects to which I am seconded to provide security risk management advice. I have successfully applied BPSA to three major commercial

projects so far, and have others in the pipeline. One of them appears as the third case study in this report.

As a security risk manager, the project has transformed my way of working by providing an approach to assessing the security risks pertaining to any business or project without any specific prior knowledge or experience of that field. It has become the preferred approach in my company and is breaking down the barriers between the security department and wider organisation. The Affiliate managers who have worked with me have commented that they feel they now have a way of fulfilling their security risk management responsibilities which they previously lacked. I am currently working on ways of disseminating the approach to a wider audience without having to deliver it in a face-to-face setting.

Ultimately, the project has profoundly transformed my way of working and continues to do so. Most significantly, I feel I now have a means of protecting *business processes* and thereby the businesses themselves, rather than simply the *locations* where business takes place, the *people* who carry out business tasks or the *equipment* and other resources they use.

Report structure

The next chapter presents my literature review. I have been as concise as possible, but it is necessarily detailed because my approach to the project demands an extensive took-kit of concepts and theories to be used as needed. I profess few theoretical loyalties and am happy to reject a preferred theory in favour of one I am normally critical of, if the circumstances appear to demand it. I have therefore provided an overview of the subject domains that I carry around with me and refer to in whatever depth or detail I see fit.

This is followed by chapters on my research ethics and positionality. There are also many ethical challenges in my role, as I often deal with whistle-blowers and other types of informant who may seek to supply information for reasons other than those they declare. However, this is part and parcel of working in the security and investigations professions and nothing about my project made this any more or less challenging than normal.

My positionality chapter presents a biographical account of my life experience before I joined the security world and considers how this has shaped my professional persona. I also reflect on my role as – for the most part – an organisational insider. Although any work-based project is likely to entail a significant amount of insider perspective, I found that I shifted between insider and outsider depending on my familiarity with the local team, the role I had to play – i.e. investigator or advisor – and a wide range of other variables that coloured my experiences of interaction and observation. One of the project benefits was to make me more sensitive to this flux when I now encounter it.

The next chapter presents my methodology which is structured as a narrative of how my ontological and epistemological stance evolved over the project's duration. Having started as a mixed methods approach that was firmly rooted in positivism with a few qualitative embellishments, I moved to a more interpretivist approach in a case study framework using a bricolage of group work, interviews, observations and role-play. My analytical framework was derived from sensemaking and adapted to the theoretical framework which I present in my literature review.

The chapter that follows presents the case studies. These are arranged in chronological order to demonstrate how my approach developed over time and grew from something very specific to security into a more holistic, multi-disciplinary toolkit. The case studies I've chosen are from a range of industries, including minerals, automotive and textiles and from regional settings in Latin America, Eastern Europe and North Africa.

My conclusion summarises the project and the report's chapters, then argues that security risk management is not best achieved by abandoning it to the experts. It does need to be integrated in mainstream management practice and culture, and the Business Process Security Analysis approach presented in this project offers a good approach towards achieving this.

CHAPTER 2: ETHICS

This report deals with commercially sensitive issues so, to limit the possibility of identification of any individual or company, I have anonymised the names, company names, locations and even the specific countries where the research took place and requested the report be embargoed for a period of two years.

Although pursuing a doctoral qualification benefits me personally and professionally, the successful delivery of the project required it to achieve benefits for my company (who funded my participation in the programme) and eventually, the body of knowledge in my chosen field of study. My project was designed and conducted to be in the company's interests so at no time did I need to gather information outside of these parameters. Managers in the various locations where I conducted my research were informed of these aspects and fully supported them.

It is also important to recognise the potential for my role to have a significant and potentially life-changing impact on other employees – especially those who become suspects in investigations. However, this potential exists anyway, regardless of my engagement with this doctoral project, because it is part of my role to investigate and understand the causes of security incidents. My project neither increased nor reduced this and, if anything, formulating a more proactive and preventive approach to security helps to protect everyone in the organisation both from being victimised *and* the temptation to offend.

The corporate security function is a manifestation of an organisation's right to protect itself from security threats, so long as it operates within both the law and accepted ethical standards. These standards are enshrined in the company's Integrity code, which applies to myself and all other employees and which requires us to attend annual refresher training on integrity matters.

Participation and informed consent

Most of the focus groups and interviews that generated data for this project were conducted in the context of security risk assessments, rather than security investigations. All participants were informed of my purpose and intentions with an opening statement:

> I work for corporate security – a small team that works across all businesses and functions in all territories where the company operates. We report to the Senior Vice President for Compliance who is also the head of the global legal function. You have been invited to contribute to a security risk assessment of this [branch/project/business] which aims to identify ways of improving the personal security of employees, minimising losses through crime and negligence and contributing to enhancing the quality of our service to customers. This is your opportunity to be heard, so please feel at liberty to speak openly. If you have any information or even just an opinion that you wish to share in confidence, you can either approach me directly, contact me by telephone or email, or use the company's Compliance Hotline which is totally anonymous and is open 24-7. However, our purpose here and now is to share information among ourselves so that we can try to improve conditions for all.

In the case of formal investigations, no employees are legally obliged to be formally interviewed by corporate security and we have no powers of detention or compulsion. Although they would probably be in breach of their general conditions of employment to simply refuse to assist an investigation, there is nothing to stop them insisting on legal representation while they do so or simply leaving the premises.

Deception

Security operatives occasionally use techniques of deception, such as pretext calls (where the caller assumes a false identity to conceal the purpose of their enquiry), covert surveillance or interception of communications, but none of these techniques were needed or used during this project.

Debriefing

All managers and employees had recourse to complain if they are dissatisfied with any aspect of their encounters with members of my department. We are wholly accountable for our actions and will refuse to carry out illegal or unethical instructions.

To summarise, my project absolutely complied with all these norms and none of my research activities compromised them. In some cases, my analyses helped to identify unacceptable exposures of personnel to security vulnerabilities, enabling corrective actions that helped ensure their personal safety and vulnerability to temptation. Indeed, my project focuses attention on the importance of system design and management awareness of risks, as well as the importance of personal comportment.

Even now at the time of writing, I am preparing for my next project which will be to transform the company's current model of integrity as an essentially personal and individual challenge, to one that must be integrated into the practices, procedures and performance measurement of the management structure. This will hold managers accountable and may even exonerate lower level employees from disciplinary action if it can be shown that their behaviour is more a product of leadership culture than individual choice.

In summary, my ethical position on security is that it is as much about protecting people from unacceptable organisational pressures as it is about protecting organisational assets from conscious wrongdoing by employees. At no time during my field research were any ethical values compromised in any way.

CHAPTER 3: POSITIONALITY

My positionality in this project is a product of my history, identity and evolving world-view. Some aspects are a product of personal decisions and conscious choice, while others are revealed by reflection. The importance of positionality is well expressed in the following:

> The nature of qualitative research sets the researcher as the data collection instrument. It is reasonable to expect that the researcher's beliefs, political stance, cultural background (gender, race, class, socioeconomic status, educational background) are important variables that may affect the research process. Just as the participants' experiences are framed in social-cultural contexts, so too are those of the researcher.
>
> Bourke, 2014: 2

Writing of ethnography from a realist perspective, Hammersley and Atkinson (2007) note that we are part of what we observe and that we cannot avoid:

> … having an effect on the social phenomena we study. In other words, there is no way we can escape the social world to study it.
>
> Hammersley and Atkinson, 2007: 16

Reflecting on my project while analysing my data and particularly while writing this report, I came to recognise that, in addition to offering myself as the 'data collection instrument', I was also at least part of the *research subject*. Decoding and reflecting on my own thinking, actions and analysis – not least, to assess the extent to which I may reasonably codify them for use by others is an important component of this work. I examine these in the context of the setting, my role at that time, which is partly determined by the instructions I have received, and how I am regarded by others while I act *in that setting* and *at that time*.

Positionality is not biography but 'positionality *and biography* directly affect fieldwork' (England, 1994: 80, emphasis added) so I will share some of my personal history here. My father was a police officer, so I grew up in a law enforcement environment and recognise that this had a lasting influence on me. However, I rebelled and dropped out when I was 17 and bought a one-way bus ticket to Spain, where I played in a professional rock band for several years. Much of this time was spent somewhere between decadence and utter poverty and I was very lucky to avoid disaster. I returned to the UK and was offered a job as a music teacher and care worker in a therapeutic community for emotionally disturbed adolescents. Up to this point in my life, I knew a thing or two about taking risks and 'thinking different' but I was completely immersed in the arts and was starting to feel limited by them. I had also had the luxury of only really having to think about myself, which was about to change.

After five years of working with kids who had suffered incredible abuse and depravity, my worldview started to change and I got interested in security issues. I also wanted to expose myself to risk, so I considered a military career and had conversations with the British Army Intelligence Corps. Eventually, this didn't work out, so I went to Marseilles to decide whether I should join the French Foreign Legion. Although I was seriously interested, I decided that I would not achieve a life of adventure and self-discovery (which was what I think I sought) by that means, so I got an education instead.

I became an undergraduate student at 29, reading for a degree in English and American Literature from which I graduated with first-class honours. Having thoroughly enjoyed the academic

experience of my degree, I then enrolled in the MSc in Security Management and Information Technology at Leicester University's Centre for the Study of Public Order (now Department of Criminology). I do confess to being as intrigued and attracted by the name of the institution as I was by the subject matter. Like most of my decisions in younger life, applying to join the course had more to do with my aesthetics and sense of curiosity than making sensible career choices. I had no plan, but I did feel a calling.

The course was one of several that started to appear around that time that were funded by the government to encourage the professionalisation of various emerging disciplines – one of which was security management. The parameters and construction of this discipline is discussed in more detail in the next chapter, but the course was taught as a combination of criminology, management theory and the use of information technology (e.g. SPSS) to analyse social scientific data. Essentially, it proposed that we cannot manage security unless we understand the nature, cause and scale of the behaviours that threaten it, and the structure, culture and other aspects of the organisation we aim to protect. Writing now, over 25 years later, I still believe this essential proposition to be the right one and can confirm that it has continued to influence my perspective throughout my career.

I spent the next ten years as an academic researcher and lecturer at that same university. I worked on various research projects on both public and private security and the relationship between the two in Europe, the USA, China and Brazil. This provided me with opportunities to explore my subject at an international level and to publish in the most prestigious academic journals in my field. While I would characterise my research position at that time as an 'outsider looking in', I instinctively strove to break down barriers and gain as much understanding of the 'insider' perspective as I could. I felt compelled towards trying to understand the world as it appeared to those whose work I was studying. This is an impetus that I continued to invoke in my subsequent career and especially in my project while trying to empathise with colleagues with ontologies and epistemologies derived from the natural sciences, engineering, technology and other backgrounds that differ from my own.

However, as I will discuss further in my Methodology chapter, my research training and orientation was firmly anchored in a positivist ontology. I started to experiment with participant observation to achieve greater depth of insight and sought to immerse myself as fully as possibly in the professional cultures and sub-cultures of my research populations. Reflecting on these experiences now, I see them as something I did primarily to complement the quantitative approach that seemed to dominate the research culture in my field. However, it is also possible that I was instinctively seeking some sort of mechanism to pull me back into a people-centred perspective on my subject, i.e. one that focussed on and celebrated the human experience.

I also very much enjoyed this depth of engagement. An unintended product of my participant observer experiences was a renewed appetite for the practitioner experience, so I left academic life to work as a consultant. In this role, I carried out professional research using many of the tools I had acquired while studying and working at the university, yet I started to augment these with other techniques that I had learnt from my earlier observational studies of police and security practitioners. I conducted covert observations of illicit markets in the *favelas* of Rio de Janeiro and

São Paulo, and similar locations in Santiago de Chile, Mexico City, Budapest, Moscow and St Petersburg. I conducted physical 'penetration tests' of secured facilities, including banks and other institutions to find opportunities to cause mayhem ('thinking criminal') and then to improve security. I also got involved with intelligence analysis and participated in training missions for government in Pakistan and for private interests in South Asia and South America. Later, I had an occasional role as a Consultant Advisor to a Counter Terrorism Unit of the UK police, with which I developed simulation exercises that we ran for audiences of similar organisations in various countries in Europe and the Near East.

I carried my theoretical knowledge with me through all these experiences and, even though I had left academic employment, I still sought out opportunities to reflect and occasionally publish in scholarly journals (e.g. Hart, 2010) or speak at conferences when the subject matter allowed. I was also prepared to go anywhere in the world with 48 hours' notice, so long as I had a visa and life cover to protect my family.

The product of this diverse approach to my career was a niche profile that, while unconventional, is respected in my field. When invited to speak at the Association of Security Consultants' annual conference in 2016, I was introduced as a 'pracademic', meaning someone who actively maintains a relationship between the theory and practice of my discipline. I took this as a compliment and acknowledgement of my efforts to use one to explore the other over many years, although I suspect such a descriptor would not be used for a member of the established professions (e.g. law and medicine) whose traditions may require them to engage continually with new knowledge and to integrate it into their practice. I see no reason why such expectations should not apply to new and emerging professions, such as my own.

The security profession used to be dominated by former police and military practitioners and my early attempts to enter it at the level I wanted to work at were frustrated by my lack of such a background. I had to reinterpret and reconstruct my experience as well as to gain new competences and skills to enable me to compete in the *market* in order to contribute in the *field*. I enlisted in the professional doctorate programme because I wanted to consolidate my career with a doctoral qualification and I chose this project to explore and present my approach to security risk management in a form that will benefit my company, as well as other organisations and practitioners when I publish some of it.

My current job title is Global Security Risk Manager and, while my role focuses on helping the company prevent security incidents (which requires research and analysis), I am also called on to investigate them and contribute evidence to any consequential disciplinary processes.

During both the conduct of my research and in my work in general, I find that my perspective shifts between three personas:

- Observer and learner (outsider)
- Trainer and advisor (insider)
- Protector, investigator and enforcer (insider/outsider)

Which of these emerges first or dominates a piece of work or case study depends a great deal on the reason for my involvement. During my project research, I was unable to exercise total freedom

over which parts of the business I studied and which persona I had to adopt at any given moment, and therefore had to adapt to the circumstances my job compelled me to find myself in.

Observer and learner (outsider)

If called in to advise and assist – perhaps in the wake of an incident that had already been dealt with by others – then the role of outside observer came naturally. As I commenced my research just over a year after commencing my employment, I was then and still am now in a state of continuous learning about new services and settings. Even at the time of writing, over seven years after joining the company, I am frequently surprised to discover new business activities or services that I had no previous idea we offered, so my job requires me to be actively engaged in continuous learning. This also requires me to build close relationships with those who possess the knowledge and expertise to help me learn – and to become an insider.

As I reflect on my project, it occurs to me that the insider-researcher lacks some of the privilege of the outsider invited in, which is the usual role I had in previous projects. While the outsider faces other restrictions, my experience is that the research process is more orderly: disruptions occur, but for different reasons. The role of the outsider-researcher is accepted as being present to conduct research, while the insider-researcher cannot easily detach themselves from or neglect their core role.

Trainer and advisor (insider)

I design and deliver various training and education initiatives to engage non-security practitioners in my subject, yet training and advising often takes less structured forms and take place within the kinds of group work that formed part of this project.

Protector and enforcer (insider/outsider)

The protector role involves applying my expert knowledge and combining it with the expertise of others to design the most efficient and effective approach to business enablement that can be achieved in the relevant circumstances and setting. Here, I begin as an outsider but work my way in to the inside by listening and sharing and otherwise building trust so that my input is perceived as valid and results in action – for example, by service designers.

In contrast, the ‘enforcer’ role must retain an outsider perspective and is that most closely related to police work. Colleagues encountered in the other forms of interaction could easily become suspects or their associates, or they could be instructed to avoid sharing insights or information with me to protect the status quo.

In theory, an unscrupulous security practitioner could exploit such a position as mine, including for the purposes of furthering a research agenda. However, as my project focussed on processes, dynamics and abstract concepts, there would have been little or no benefit to derive from such behaviour and it would cause harm to myself and others.

In addition to identifying any guilty parties who may be selected for disciplinary action, including termination, my security investigations focus on the circumstances and systemic failures that allowed the security breach to occur. My primary interest is how this knowledge can be used to inform future prevention to protect people and enhance business performance. While security

advice could include recommendations to end projects or close businesses, with adverse consequences for employees' job security, this would be a result of neutral observation of the associated details and not any separate activity related only to my academic research. However, I have had the experience of redundancy while maintaining a home and family, so I take an organisation's responsibilities to provide sustainable prosperity to its hard-working members very seriously.

CHAPTER 4: LITERATURE REVIEW

Writing from an insurance perspective, Van Oppen defines *risk management* as 'the systematic, positive identification and treatment of risks posing a threat to values (or resources) of human concern' (Van Oppen, 2001: 2). Earlier, I defined security risk management as 'a management discipline and organisational function that integrates assessment of the threat of *intentional* harm with the implementation of strategies, tactics and techniques to reduce both the probability and impact of harmful acts'. My added emphasis on the word 'intentional' highlights the need to respond to the free will and creative effort of individuals and groups who act with a purpose. The harm that security risk management addresses is not the result of an accident or mishap.

As a subject and as a practice, security risk management draws from many disciplines and combines a wide range of ontologies and epistemologies that allow equally wide interpretations of the key concepts embedded within it. This chapter aims to present a review of the literature that constitutes the academic part of my epistemology within my wider professional praxis. My aim is to try to summarise the knowledge-base I refer to in my work in general and also present the way I and others like me work within a wider context of *policing*. The three main subject areas covered in this literature review also provide the primary analytical framework I use for the case studies.

The chapter is structured to address the concepts of security and risk in turn, before offering my view of security risk management and corporate security as the operating framework within which this knowledge is applied.

The study of security provides access to technical knowledge about the techniques of crime prevention, as well as a more social scientific epistemology about the causality of security threats. It is this – a form of applied criminology – that is of greatest relevance to my project as it concerns the characteristics of the offender and the target for attack, as well as the environmental and situational characteristics where they converge.

The study of risk explores how we deal with uncertainty and the strengths and weaknesses of various approaches to understand it and make it manageable. This part of the chapter critiques (but does not *reject*) the established view that security risks are, like temperature or volume, somehow measurable – while maintaining that the techniques for doing so are still useful when appropriate. A social scientific perspective and cultural theory of risk are also explored.

The third section presents security risk management as a fusion of these disciplines with various management and organisational theories that also may have a causal effect on security risks, as well as indicating the practical pathways we can follow to understand them as part of the organisational experience, as well as manage them. This section also addresses existing security risk management frameworks and explores why they did not meet the needs that I encountered in my organisation.

Security

A state of being

Security is an existential necessity. Etymologically derived from the Latin *se* meaning 'free from', and *cura* meaning 'care' or 'worry', it is 'the state of being free from danger or threat' (Oxford

English Dictionary, 2017). Every species of plant or animal has evolved techniques to ensure their security, including defence against known predators, and human beings are no exception. In his famous model of human motivation, the 'hierarchy of needs', Maslow (1943) ranked security and safety as above the need for love or esteem and second only to physiological necessities, such as air, water and food. Along with *human rights*, *rule of law* and *development*, the United Nations defines *peace and security* as one of its Four Pillars, with the aim of facilitating security for all people (United Nations, 1945). A World Bank study that sought 'to gather the views, experiences, and aspirations of more than 60,000 poor men and women from 60 countries' (Narayan, Chambers, Shah and Petesch, 2000: xv) found that security was integral to their definition of a good quality of life.

In the context of business and commerce, Fayol identified in the earliest days of management theory the provision of security ('protection of property and people') as one of six key activities of industrial organisations, while the overall quality of the most advanced technological products in the 21st century is often determined by their security-related attributes. The impact of security failures and business victimisation on the wider economy has sufficient prominence for the British Government to conduct an annual Commercial Victimisation Survey (Williams, 2016). At the international level, the global dynamics of power, struggle for economic, political and cultural dominance and the risks presented by climate change, population growth, conflict and war all lead to pressure on organisations to make informed security decisions. Security is an issue that affects us all, whether directly or indirectly, but where does responsibility for security ultimately lie?

As the needs of society, businesses and individuals overlap and intersect, the provision of security is complex and responsibility for it is not easily compartmentalised. For example, while the State is ultimately responsible for the provision of national security, the UK's National Counter Terrorism Security Office also reminds us that 'businesses and industry must take steps to protect themselves' against the threat to their security presented by terrorism (NaCTSO, 2015). Such statements and exhortations demonstrate the State's recognition that it cannot sustain a monopoly on the protection of life and property even from the threat of political violence. Private and corporate security provision is one of the ways that commercial entities accept their share of the wider burden, as well as addressing security risks that are peculiar to their activities and interests.

I will return to the *provision* of security in more detail in the third section of this chapter. First, I need to explore the theoretical underpinnings of security as a state of being, starting with the concepts of threat and intentional harm.

Safety practitioners concern themselves with identifying *hazards*, defined as 'situations with the potential to cause harm' (Royal Society, 1992: 4) that tend to be associated with accidents. As security practitioners are typically more concerned with intentional harm, they usually use the term *threat*, which is formally defined as an aggregation of *intent* and *capability* (Singer, 1958; AAAS-FBI-UNICRI, 2014). There is an intersection between the two concepts, as hazards create opportunities for threats to materialise, as illustrated by the occurrence of looting following natural disasters, but they are separate disciplines and this is usually manifested in how they are structured in organisations as well as in the skillsets and knowledgebases of practitioners. One of the key distinguishing features is the element of *intent* within a security threat. This brings with it all

the creative determination that perpetrators can muster to create and exploit opportunities, and the willingness to evade protective countermeasures by formulating new and innovative forms of attack. Security risk assessments need to be creative as well as cyclical and ongoing because threat is volatile and constantly evolving.

As one of the goals of security is to deter people from offending, it is useful to understand why they offend and what they hope to gain. Indeed, criminal threats can be classified by the motivation of the threat agent or perpetrator and vice versa. Theft, fraud, robbery, extortion and any other proscribed behaviours intended to achieve illicit gain are classified as *acquisitive* crime, while *expressive* crimes, such as criminal damage and crimes of violence are motivated by emotions, urges, beliefs and sometimes ideologies.

We can also classify threat agents or offenders in various ways. In the commercial setting, it is useful to recognise that businesses can be victimised by *external* actors, including customers, competitors or simply professional criminals, or by employees, contractors and partners who have access to the business as *insiders*. These are sometimes termed 'white collar criminals' (Sutherland, 1949) although that terminology tends to apply specifically to those in management or administrative positions with access to sensitive information and the ability to manipulate financial processes.

Threats presented by one group may not be as responsive to a given treatment as might be other threats presented by a different group with different motivation. So, to conduct a meaningful security risk assessment, it is important to understand cause, in much the same way that understanding how the cause of sickness relates to the practice of medicine. The study of the causes of crime is known as criminology.

Criminology

My discussion of criminology is intended to explore how the study of crime progressed from assumptions of a universal rationality shared by all, to a 'scientific' focus on the biological characteristics of offenders, a sociological focus on the social settings we all occupy and, eventually, the situational characteristics where acts of deliberate harm may occur.

Criminology is part of a wider *sociology of deviance* that attempts 'to explain a world of laws, rules, courts, criminals, rule-breakers, police and prisons' (Downes and Rock,1995: 27). Security risk managers can adapt its principles and theories to enhance their understanding in their domains of responsibility of how security threats are defined and what motivates their perpetrators.

Early criminology emerged during the Enlightenment of the 18th century and its principles remain fundamental to how societies and private organisations define and manage criminal or deviant behaviour within systems of justice. Philosophers such as Beccaria (1764) and Bentham (1781) explored the relationship between the individual and society and recognised the need for an effective justice system to balance the politically defined values of freedom and responsibility. This 'classical criminology' argues from the principle that individual human beings exercise free will rationally but in their own interests, so if they commit crime it is by choice and it is the responsibility of a civilised society to influence their choices with the threat of punishment to encourage them to act for the greater good. This is the 'hedonistic calculus' (Bentham, 1894:18) or pleasure-pain

principle that classical criminologists believe people refer to when weighing the 'pleasure' of acting selfishly against the 'pain' of the punishment that society will administer if they break the law. In the workplace, it is usually manifested in rules enshrined in disciplinary codes which must, of themselves, comply with the public systems of law that include the criminal and civil justice systems, as well as various regulatory frameworks.

However, the sociology of deviance questions 'the slippery notion that law is a spontaneous and uncontrived product of the continuous flow of life, made accessible to man through reason' (Henry, 2015: 1) and recognises that all rule systems protect the interests of those who create and administer them. For commercial entities, referring cases to public justice is expensive and even involving the police in an investigation can incur undesirable consequences. These arise from the inevitable loss of control of the investigation as well as the risk of unwanted public exposure which may cause further harm, including financial and reputational losses. The police are focussed on law enforcement and delivering a wider definition of justice and 'are not oriented towards recouping the losses of the company' (Lippert, Walby & Steckle, 2013: 209). They may also decline to take any action at all, if they judge it not to be in the public interest. There is also a very real risk of police collusion with criminal elements (Cooper, 2015; Stephenson, 2017) in some countries and it is my experience that many private security companies that specialist in certain threats such as extortion or kidnap and ransom, will decline business if the police have been involved.

Within the corporate domain, the rule structures that define deviance and govern how infractions might be dealt with are effectively *private* justice systems. These exist in relation to public systems in varying degrees of formality (Shearing and Stenning, 1979, 1983; Dempsey, 2008; Meerts and Dorn, 2009) and are 'supported and channelled by Government and judicial activity' (Andrews, 2008: 8) so long as their rules and actions do not violate public law or otherwise conflict with public interest. Their use is accepted for appropriate cases, not least because overuse of the formal legal process places an expensive and time-consuming drain on public resources. Indeed, public justice systems would collapse very quickly if every prosecutable case were referred to trial (Travis and Edwards, 2015: 118). Managing problems away from public justice can also benefit offenders because, although an informal resolution is likely to result in some form of sanction, e.g. termination of employment, they will avoid a criminal record as well as any negative publicity.

However, private justice systems are far less likely to be as clearly and comprehensively defined as public systems, and decisions about disciplinary actions may be arbitrary and lacking in transparency. This can present the company with legal risks, as accused individuals retain the right to seek redress via public justice and its higher burdens of proof, expensive lawyers, time-consuming procedures and public exposure. Companies know this and seek to avoid it and offenders are likely to be aware of this situation as well. Exploiting the rationalist perspective that underwrites the classical criminology perspective, determined offenders may judge the threat of sanction to lack credibility and assess the benefits of offending to outweigh the risk. It is reasonable to conclude from this that the pleasure-pain principle cannot be relied on to deter crime.

The beginnings of modern criminology saw a shift of focus from the criminal law and the bland acceptance that human beings were rational, to the criminals themselves. Abandoning the 'armchair reasoning' and philosophical reflections of classical criminology, early positivist

criminologists tried to formulate scientific explanations of why people offend, despite the threat of punishment. They produced a range of theories which argue that 'behaviour is determined by factors beyond the individual's control' (Vold and Bernard, 1986: 10) rather than personal choice and focussed first on the nature of offenders and then on the environments that produced them. This produced two types of scientific theory, which I will refer to in broad terms as *biological* and *social* determinism.

Early biological determinists – sometimes 'with a Darwinian concern with species and their evolution' (Garland, 1997: 30) – believed that criminals were physically different from the law-abiding population. They viewed crime as a behavioural manifestation of the offender's natural biological or evolutionary state, and that this explained why they were unable or unwilling to partake in the social contract. The most famous example of an attempt to 'prove' this scientifically is the work of Cesare Lombroso, an Italian army physician who conducted an empirical study of the physical and behavioural characteristics of the inmates of a military prison. He claimed his findings proved that criminals were an 'atavistic throwback' to an earlier stage in human evolution (Lombroso, 1878) but didn't take proper account of social factors that may have contributed to their misshapen bodies, such as poor nutrition, violent abuse and social depravation. In the 1930s, anthropologist EA Hooton conducted similar studies in the United States and sought to link criminal behaviour with physical characteristics, particularly those of various minority ethnic groups (Hooton, 1939) which he believed to be inherently criminal. His studies were based on comparisons between 'criminal' and 'non-criminal' groups, but he also failed to account for the many factors that challenged or contradicted his contention that criminals were biologically different (see Vold and Bernard, 1986 for a detailed critique).

Biological determinism has been exploited to justify prejudice and the marginalisation of entire social and ethnic groups. However, throughout my professional career and in this project, I have found that an awareness of such theories and the many methodological and intellectual flaws in the studies that produced them to be of value. This is not because I believe they have any validity. Rather, it is to be able to counter the extent to which they have penetrated the popular mindset and the influence they still have. While racism and prejudice against minority groups is proscribed by law and rejected by mainstream social values in most first world nations, this is often not the case in many other cultures. Negative assumptions about the criminal propensities of groups considered 'unclean', less intelligent or otherwise inferior because of their ethnicity or other inherent traits are implicit in some business and employment decisions and openly expressed in certain circumstances. Similarly, concerns about security are sometimes misappropriated to justify discriminatory practices, for example based on gender stereotyping. Women are denied certain positions of responsibility to protect their 'vulnerability', while males may be placed in risky situations because they are expected to be able to defend themselves.

This said, it would be unfair to label the entire biological perspective as an abuse of science. More recent biological explanations of criminality (e.g. DeLisi, 2012) has helped to establish mitigating factors to justify a treatment-based approach rather than the punishment-oriented model of retributive justice. Other examples draw from the various psychological traditions concerned with abnormalities of mind resulting from trauma and abuse.

Beyond the rights and wrongs of their causal explanations, we must also recognise that the empiricist methodologies that early criminologists used to reach their findings have had a profound effect on the study of crime beyond the narrow confines of individual propensity. The emergence of positivism and the elevation to primacy of the method of science as the philosophical foundation of social research also produced new forms of 'social determinism' which argued that crime is a consequence of poverty and unfair social and economic systems.

While businesses can have only limited impact on changing the social conditions that are beyond their control, recognition of the relevance of social theories to business is longstanding. In the late 1930s, leading business executive and management scholar, Chester Barnard '… in sharp contrast to the mechanistic conceptions of earlier management thinkers, such as Frederick Winslow Taylor … viewed the organization as a complex social system':

> [He] focused on the complexities of the human element in organization, on the psychological forces of human behavior, and on developing ways to manage the complexities of human behavior and to cope with its limitations (Gabor, 2000).
>
> Gabor and Mahoney, 2010: 3

In my project, I found that such 'psychological forces' and 'complexities of human behaviour' were potent inputs into how businesses really work – and how they manage security risks – even though they rarely appear on flow charts or process maps. Business organisations are micro-societies that can benefit from the application of theories developed in the wider society, and this is particularly true concerning criminality. For example, *Strain Theory* (Merton, 1938; Cloward and Ohlin, 1960) posits that people break rules as a reaction to social pressures resulting from anger at perceived injustices or feelings of relative depravation. During investigations into workplace crime, various offenders have confessed such feelings to me, citing low wages or being overlooked for promotion as motivational factors. Similarly, *Social Learning Theory* (Akers, 1979) argues that crime is learnt behaviour, acquired from peers, family or community. In the workplace setting this includes colleagues and line managers, and some work-based studies (e.g. Ditton, 1977) have found that criminal sub-cultures can become deeply embedded inside businesses. Ditton found that criminal factors also influenced recruitment decisions, as they provide informal mechanisms of discipline and control that allow managers to short-cut due process. My project encountered several examples of this phenomenon, particularly where unacceptable practices by business leaders have been allowed to continue for lengthy periods without remedial action. Criminal behaviour becomes normalised and corrupt managers may actively seek to subvert systems of control to protect their own interests and the parallel systems they have created.

Social theories of crime have been criticised, not least because of their apparent ineffectiveness when implemented:

> Once upon a time we thought that if we could only get our problem families out of those dreadful slums, then papa would stop taking dope, mama would stop chasing around, and Junior would stop carrying a knife. Well, we've got them in a nice apartment with modern kitchens and a recreation center. And they're still the same bunch of bastards they always were.
>
> Seligman, 1957: 124

Nevertheless, applied to the workplace, it is often the case that offenders who cause the greatest harm are in positions of power and privilege, rather than being among the lowest paid or

performing the least pleasant tasks. It is also true that blame falls more easily on the shoulders of someone working in an operational role than of their line management.

Social theories also remind us that achieving a state of security is also about well-being, not just deterrence and the implementation of security technology, and they provide useful insights into a range of motivational factors that must be considered in any security strategy. The combined presence of a supportive management style, opportunities for progression, positive peer culture and other factors can have a significant impact on reducing offender motivation. By establishing working conditions that are *not* conducive to criminal behaviour, we can apply social crime prevention measures in the workplace to foster a better working environment.

Applied specifically to the working environment, social theories of crime also help us select the physical location of workplace facilities and assess the risks of daily (and nocturnal) access. *Social disorganization theory* emerged from studies of the urban environment in Chicago in the 1920s (e.g. Shaw and McKay, 1942) which found that certain areas were more likely to experience criminality because of the dominant sub-cultures present. This evolved in the 1980s into environmental criminology which 'argues that criminal events must be understood as confluences of offenders, victims or criminal targets, and laws in specific settings at particular times and places' (Brantingham and Brantingham, 1991: 2). However, forms of environmental criminology such as *crime prevention through environmental design* (CPTED) (Jeffery, 1971) and Newman's *defensible space* model (Newman, 1972) have helped me recognise that premises close to shanty-towns and 'red light' areas can also sometimes benefit from the proximity of friendly neighbours providing informal surveillance.

Broken windows theory (Wilson and Kelling, 1982), although conceived from an opposing political perspective, also argues that social evidence such as vandalism and litter indicate that criminality is considered acceptable and therefore more likely to occur. I have used this reasoning to insist on prompt damage repairs and graffiti removal as soon as it happens, as this sends a clear signifier that the facility is cared for and that offending behaviours are unlikely to be tolerated.

The next set of theories I want to discuss continues the shift of focus away from the biological and sociological characteristics of the offender or their social setting, to those specific to the situation where a security breach may take place. Such theories of crime offer a strong theoretical basis for treating the environment as a causal factor, and reducing the risk of crime by changing aspects of the setting to influence the offender's decision-making.

Returning to and drawing from the rationalism of classical criminology, the *Rational Choice Perspective* of James Q Wilson (1983) argues that offender decision-making is based on a rational and intelligent analysis of opportunity:

> At the heart of rational choice is an analysis of the thought or cognitive means by which individuals process information from the environment. Rational choice theory focuses on the individual offender's perception of the opportunity structure of each environment and his decision to maximise gain and minimise loss from the environment.
>
> Jeffrey and Zahm, 1993: 337

Various opportunistic theories have emerged from this perspective which are easily applied in practice. *Routine Activities Theory* contends that crime occurs when there is a 'convergence in space and time of the three minimal elements of direct-contact predatory violations: (1) motivated

offenders, (2) suitable targets, and (3) the absence of capable guardians against a violation' (Cohen and Felson, 1979: 589). Clarke (1997) argues that most criminological research failed to consider the second two of these elements and that 'the problem of explaining crime has been confused with the problem of explaining the criminal':

> Most criminological theories have been concerned with explaining why certain individuals or groups, exposed to particular psychological or social influences, or with particular inherited traits, are more likely to become involved in delinquency or crime.
>
> Clarke, 1997: 2

His *Situational Crime Prevention Theory* focuses 'on the settings for crime, rather than upon those committing criminal acts' (Clarke, 1997: 2) and proposes that, regardless of other influences on offenders' behaviour, applying measures to *increase the effort* they must exert (Felson and Clarke, 1998); *increase their perception of the risk* of detection (see also Gill, 1998); and *deny the benefits* of crime to offenders by designing assets in such a way as to render them useless if misappropriated (Clarke, 1997). The theory evolved into 25 techniques which the following table presents with some common examples of their implementation (Cornish and Clarke, 2003: 90):

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
1. Target harden • Steering column locks and immobilisers • Anti-robbery screens • Tamper-proof packaging	**6. Extend guardianship** • Take routine precautions: go out in group at night, leave signs of occupancy, carry phone • 'Cocoon' neighbourhood watch	**11. Conceal targets** • Off-street parking • Gender-neutral phone directories • Unmarked bullion trucks	**16. Reduce frustrations and stress** • Efficient queues and polite service • Expanded seating • Soothing music/muted lights	**21. Set rules** • Rental agreements • Harassment codes • Hotel registration
2. Control access to facilities • Entry phones • Electronic card access • Baggage screening	**7. Assist natural surveillance** • Improved street lighting • Defensible space design • Support whistle-blowers	**12. Remove targets** • Removable car radio • Women's refuges • Pre-paid cards for pay phones	**17. Avoid disputes** • Separate enclosures for rival soccer fans • Reduce crowding in pubs • Fixed cab fares	**22. Post instructions** • 'No Parking' • 'Private Property' • 'Extinguish camp fires'
3. Screen exits • Ticket needed for exit • Export documents • Electronic merchandise tags	**8. Reduce anonymity** • Taxi driver IDs • 'How's my driving?' decals • School uniforms	**13. Identify property** • Property marking • Vehicle licensing and parts marking • Cattle branding	**18. Reduce emotional arousal** • Controls on violent pornography • Enforce good behaviour on soccer field • Prohibit racial slurs	**23. Alert conscience** • Roadside speed display boards • Signatures for customs declarations • 'Shoplifting is stealing'
4. Deflect offenders • Street closures • Separate bathrooms for women • Disperse pubs	**9. Utilize place managers** • CCTV for double-deck buses • Two clerks for convenience stores • Reward vigilance	**14. Disrupt markets** • Monitor pawn shops • Controls on classified ads. • License street vendors	**19. Neutralize peer pressure** • 'Idiots drink and drive' • 'It's OK to say No' • Disperse troublemakers at school	**24. Assist compliance** • Easy library checkout • Public lavatories • Litter bins
5. Control tools/ weapons • 'Smart' guns • Disabling stolen cell phones • Restrict spray paint sales to juveniles	**10. Strengthen formal surveillance** • Red light cameras • Burglar alarms • Security guards	**15. Deny benefits** • Ink merchandise tags • Graffiti cleaning • Speed humps	**20. Discourage imitation** • Rapid repair of vandalism • V-chips in TVs • Censor details of modus operandi	**25. Control drugs and alcohol** • Breathalyzers in pubs • Server intervention Alcohol-free events

Radical *Left Idealist* or Marxist criminologists (e.g. Taylor, Walton and Young, 2013) accuse the rational choice perspective of shoring up the capitalist system under the guise of preserving a

natural order, because it doesn't question the vested interests of those who define what is crime and what isn't. However, there is no reason why situational crime prevention and routine activities theories cannot be used alongside social depravation theories to help protect employee conditions and hold managers to account for their decisions. Security risk management can be as much about the protection of people and their livelihoods as it is the protection of company assets and functionality.

It is also alleged that implementation of situational crime prevention and other opportunistic theories displaces crime to more vulnerable targets – such as the homes of poorer citizens – that have not been 'treated' with situational measures. Displacement is a critical issue to consider in the commercial setting because every protective intervention can displace the threat it seeks to treat and generate new opportunities for offending that may not be foreseen at the time. Ill-considered interventions can also motivate offenders to use more extreme methods, such as attacking an individual to gain access to facility, rather than attacking the 'bricks and mortar' of the facility itself. My use of the systems approach helps address such risks by identifying targets that may be likely to suffer displacement attacks, enabling the implementation of a more comprehensive and proactive treatment.

Situational measures must be directed at highly specific forms of crime (Clarke, 1997: 4) not just broad categories such as fraud or robbery. This is because there are many nuances to do with target selection, access to the situation's location, access to a means of disposal (e.g. to convert goods into cash) and so on. This speaks to the point I made in the introduction about the pitfalls of one-size-fits-all approaches, as one of the challenges I faced in the many complex workplace situations where I conducted my research, is that I had no prior access to the relevant *crime scripts* (Borrion, 2013; Haelterman, 2016). Drawing from the language of theatre:

> [A] script describes the relation between *casts* (also called actors or roles), *props* and *locations* in a sequence of *actions*, so to characterise routines occurring in specific scenes. In a script, casts and props represent the individuals and objects involved in the behavioural process considered.
>
> Borrion: 2013

In my project, I often did not know how to recognise, analyse and understand the unfamiliar situations I encountered in sufficient detail to be able to identify criminal opportunities. In previous research (e.g. Hart, 2004), I used ex-offenders as a source of insight, inviting them to explain their rationale for target selection and their responses to security measures. This is a tried and tested method that has revealed offender perspectives on burglary (Bennett and Wright, 1984), retail theft by staff and customers (Beck and Willis, 1995) and commercial robbery (Gill, 2000) – all of which have yielded invaluable data. I did interview a small number of offenders during my project while conducting concurrent investigations, but I had to rely on the input of process owners and those employees who worked closest to a perceived risk to learn from their knowledge and perspectives. In addition to providing information about identifiable vulnerabilities, this process also gave me insight into the risk perceptions of professionals working within different disciplines. I will discuss the importance of risk perception in more detail in the next section.

In summary, this section has explained the limitations of the deterrent effect of the threat of sanction, and explored the strengths and weaknesses of causal theories that focus on the offender or their social background. These concern issues that are usually beyond the organisation's control

in terms of formulating preventive strategies, although they provide useful insights into the importance to security of managing workplace conditions and treating people fairly. My review also presented a more recent set of rationalist explanations that focus on the characteristics of situations where security threats may materialise. Although there are limitations, organisations are normally able to exert far more control over the situations where they conduct their operations than any other aspect, so situational crime prevention and rational choice theories are popular and useful tools for security risk managers. They can be applied both as an aid to analysis and as a source of ideas for preventive action in the form of security risk management.

The next section considers what is risk, if it exists in any objective sense and if it is amenable to being managed and measurably reduced.

Risk

The late 20th century saw the emergence of the 'risk society' as a major influence on intellectual, political and business thinking. German sociologist Ulrich Beck wrote that, in contrast to earlier periods, '[in] advanced modernity the social production of *wealth* is systematically accompanied by the social production of *risks*' (Beck, 1992:19). British sociologist Anthony Giddens proposed that these 'manufactured risks' produced by human activity had surpassed 'external risks' such as those presented by nature (Giddens, 1999) and that had dominated previous periods. Regarding my project, the crucial implication of these combined perspectives is that risks – at least those generated by human beings – can be identified, managed and controlled.

Risk is related to performance and achievement, but these concepts are highly contingent on organisational mission – the way it defines its reason for existence – not to mention the 'risk appetite' of managers and other key influencers. As acknowledged by The Campbell Institute:

> ... risk perception, or the ability to discern risk, is tied to risk tolerance, or an individual's capacity to accept a certain amount of risk.
>
> The Campbell Institute, 2014: 2

At the societal level, 'understanding risk and how it is perceived is a crucial step toward creating programs and campaigns to raise awareness and make communities and workplaces safer' (The Campbell Institute, 2014: 2). The critical importance of understanding risk in the workplace environment is similarly emphasised by all public, commercial and industrial sectors. For example, a joint report by the Association of Insurance and Risk Managers (AIRMIC), the public sector risk management association (ALARM), and the Institute of Risk Management (IRM) states:

> For all types of organisations, there is a need to understand the risks being taken when seeking to achieve objectives and attain the desired level of reward. Organisations need to understand the overall level of risk embedded within their processes and activities. It is important for organisations to recognise and prioritise significant risks and identify the weakest critical controls.
>
> AIRMIC, ALARM and IRM, 2010: 2

But what is risk? Beyond the deceptive certainty of the pronouncements of government and professional organisations, there is a fervent discussion about whether risk exists in any objective sense, or solely within the *risk perception* of the beholder.

Most of the scholarly literature on risk approaches the subject from three broad perspectives that emerge from different assumptions, worldviews and methodologies that form what has been

referred to as the 'risk archipelago' (Jones and Hood, 1996: 3). For ease of reference and discussion, I characterise these as:

- An 'engineering' or natural science perspective, which views risk as an objective reality that can be measured if the right tools are available or can be developed
- A predominantly psychological perspective, which focuses on the difference between the subjective perception of risk by individuals and the objective 'reality' of risk claimed by natural science
- A mainly social scientific perspective and cultural theory of risk, which defines it as a social or cultural construct that is resistant to measurement in the way proposed by the other two perspectives

Pragmatically, all three provide useful tools for assessing and managing risk in the wide varieties of ways it emerges. Further, they provide the risk practitioner with diverse ways of engaging meaningfully with stakeholders from disciplines with ontologies and epistemologies that may be more receptive to any one of the three perspectives. I will discuss each perspective in turn.

Engineering perspective

The International Standards Organisation – in what is now the recognised standard for risk management – defines risk as 'the effect of uncertainty on objectives' (ISO31000: 2009). This carries a faint echo of the earliest mention of risk in business literature, which defines it as 'measurable uncertainty' (Knight, 1921: 233) while allowing the word 'effect' to soften the certainty of the word 'measurable'. Reducing uncertainty is a perennial goal of business, and anyone who works in risk is likely to experience considerable pressure to articulate the concept using the language of certainty – most typically, in numbers. By applying the ontologies, epistemologies and methodologies of natural science to produce what it believes to be an objective and rational analysis, the engineering perspective views risk as a measurable or calculable phenomenon.

The Royal Society – the UK's most eminent scientific body – defines risk in formulaic language as 'a combination of the probability or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence' (Royal Society, 1992: 4). Like temperature or pressure, it can be *measured* or *calculated* by suitably qualified experts, then expressed in quantitative terms:

> Engineers attempt to quantify the risk by a physical appreciation of possible failure mechanisms or modes and their analysis.
>
> This requires quantification of the reliability of the components and the examination of the systematic failure ... to establish the overall reliability of the complete system, based on experience verified by analysis, testing and inspection.
>
> All systems have a probability of failure and the complete avoidance of all risk of calamitous failure is not possible, but the objective of engineers must be to reduce the probability to an acceptable individual and societal risk.
>
> Royal Society, 1992: 13

The engineering approach also dominates much of the technical literature on security. For example, writing specifically for security managers and using similarly formulaic, mathematical language, Vellani states:

> Risk is a function of threats and vulnerabilities. It is the possibility of asset loss, damage, or destruction. Risk is the result of the likelihood that a specific vulnerability of a particular asset will be exploited by an adversary to cause a given consequence.
>
> Vellani, 2006: 110

The relationship between the effect or consequences of a risk event and the probability of it occurring is indeed often expressed in formulae, such as 'Risk = Impact x Probability x Vulnerability' (Vellani, 2006: 10). Vulnerability – usually meant to express the remedial effect of countermeasures or controls – is sometimes incorporated into probability to make the formula simpler and easier to express in a two-dimensional chart.

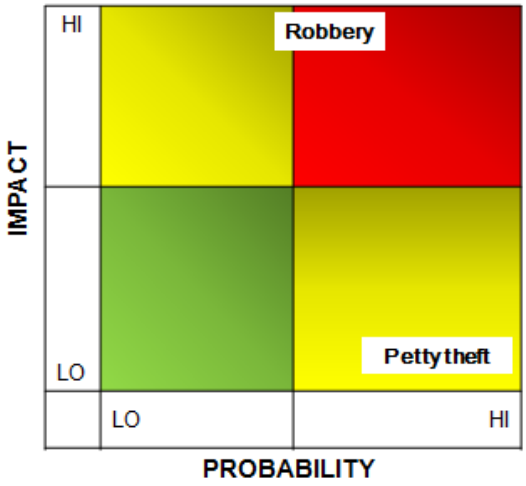


Figure 1: A Security Risk Matrix

Some risk events may be perceived to be highly probable but of low impact, vice versa or somewhere in between. Risks ranked highly along both dimensions demand urgent mitigation – sometimes referred to as 'treatment', lending a certain medical tone to the risk management process. In the example of a security risk matrix shown Figure 1, 'robbery' is deemed to be a serious threat to the business and is of above average probability which puts it in the 'high risk' red square. In contrast, 'petty theft' is seen to be of higher probability but less impact, which puts it in the 'medium risk' yellow.

The numerical values used to position risks on a matrix are typically either drawn from statistical data on previous incidents or based on some kind of scale of human estimation (e.g. the Likert 'on a scale of 1 – 5, how likely is it ...?'). Adams (1995) is critical of this process:

> Virtually all the formal treatments of risk and uncertainty in game theory, operations research, economics or management science require that the odds be known, that number attachable to the probabilities and magnitudes of possible outcomes. In practice, since such numbers are rarely available, they are usually assumed or invented, the alternative being to admit that the formal treatments have nothing useful to say about the problem under discussion.
>
> Adams, 2000: 25-26

Risk matrices have been criticised for 'fundamental mathematical and logical limitations' and because 'there has been very little rigorous empirical or theoretical study of how well risk matrices succeed in actually leading to improved risk management decisions' (Cox, 2008: 498). Even the Royal Society's scientists acknowledge the limitations of their approach:

> The results of such a procedure will be subject to substantial uncertainties arising from inadequacies in the data and from insufficient depth or accuracy of the scientific knowledge applied.
>
> Royal Society, 1992: 14

In their defence, some commentators argue that the maths is metaphorical and to be taken figuratively. However, the preference, even *demand* for numerical data – particularly in some professional cultures – 'undoubtedly reflects human preoccupation with rending the future calculable and knowable ... thereby reducing feelings of helplessness' (Hood and Jones, 1996: 84).

This said, and continuing the medical analogy from the word 'treatment', it is also important to remember that neither is medical diagnosis a precise process. In recognition of its 'error-laden' nature, Paget (1988) observes that 'the work unfolds as a series of approximations and attempts to discover an appropriate response' (Paget, 1988: 143) and this description closely approximates the reality of security risk assessment. However, detached from the context of their use as a 'guide' or thinking tool in the field, and transferred to the rarefied atmospheres where budget and resource allocation decisions are made, risk matrices and similar models can be taken too literally.

There are other methods of quantitative risk assessment and Cohen argues that they offer 'where available and appropriate, a necessary input into risk decision making' (Cohen, 1996: 87). Yet he readily concedes that they 'cannot *determine* decisions about risk, which are essentially political (Cohen, 1996: 98, emphasis added). This is a reasonable position in response to the philosophical arguments about the validity of quantitative approaches that will follow shortly, but also that highlights an important practical problem. Numerical data on security incidents in many organisations – including my own – is (thankfully) rare because we suffer relatively few attacks. This could, of course, reflect low reporting trends. Nevertheless, there is an important discussion about the extent to which analysing data concerning historic events can indicate what may happen in future.

Although the various deterministic theories may imply otherwise, there can be little doubt that criminal behaviour is at least in part a product of human creativity – even ingenuity – as well as the exploitation of opportunity, as discussed in the previous section. Predicting the next criminal trend is no easy feat and unlikely to be achieved by statistical analysis. A similar critique applies to estimating *impact*, as the effects of major incidents, such as wars and plagues are felt for years, decades – even centuries after they occur. How can we hope to know the 'magnitude of the consequences' of such events?

Most of the literature concerning the engineering approach to risk focuses on safety issues, such as chemical spills, building collapses, weather incidents or road traffic accidents, so the significance of the application of free will and human ingenuity may not be as acute as in security incidents. While safety risks are more likely to include scientifically measurable variables, such as combustibility, explosiveness or rate of diffusion, security risks are very difficult to quantify using the engineering perspective because it is not possible to quantify the unknown intentions of the threat agent, i.e. the offender and their creative ability to exploit vulnerabilities that others fail to perceive.

Psychological view of risk perception

Alongside the engineering approach exists a scientific recognition of the importance of risk perception and this was included in the original Royal Society 1983 report. However, the associated discussion and analysis was later criticised in the 1992 edition as 'dominated by economics and psychology' (Royal Society, 1992: 112) with insufficient recognition of social scientific perspectives that took a radically different and increasingly mainstream view of risk.

Consistent with the 'Newtonian' perspective on objective reality that I will discuss in the next chapter, the psychological view of risk perception shares in common with the engineering perspective that 'if risk assessment is to be more than an academic exercise, it must provide

quantitative information' (Royal Society, 1992: 83). Hood and Jones somewhat mockingly summarise this thesis as follows:

> ... both risk, and human behaviour in relations to risks, are objectively discoverable by orthodox canons of science, and the results, wherever possible expressed in numbers, are capable of being fed back into enlightened policy-making in the form of rational decision criteria applied by experts.
>
> Hood and Jones, 1996: xi

Crucially, the report and the dominant establishment view it represented continued to distinguish between the *objective risk* of 'the experts' (Adams, 2000: 7) and the *subjective risk* perceived by the lay person.

The psychological approach to risk has made extensive use of experimentation comparing (allegedly 'incorrect') human perceptions of risk with what it continues to regard as the (purportedly 'correct') 'objective reality' of risk. Among other issues, an influential study in 1978 sought to establish whether 'people have a consistent internal scale of frequency' (Lichtenstein, Slovic, Fischoff, Layman and Combs, 1978: 551) regarding fatal risk events. The authors interpreted their findings to indicate that:

> … people do not have accurate knowledge of the risks they face' and that they need to be 'corrected [by] public education … before we can expect the citizenry to make reasonable public-policy decisions about societal risks'.
>
> Lichtenstein, Slovic, Fischoff, Layman and Combs, 1978: 577

This brazenly elitist perspective may seem arcane today, although the authors acknowledged at the time of writing that experts are not immune to their own forms of bias. This has a crucial bearing on many aspects of risk assessment and how the ontological and epistemological stances of decision-makers may inform their risk perception and how they perceive the assessments of others. 'Risk appetites' vary considerably between individuals, and I have observed the power relationships within organisations – particularly hierarchical ones – to have significant impact on risk perceptions. Differences of opinion can lead to disparagement and conflict, as well as settling on a consensus view that is likely to be meaningless.

As our primary concern is reducing the risk of intentional harm, another group whose perceptions of risk should be considered are the potential offenders that security managers must strive to influence to achieve a deterrent effect. As offending is an inherently risk-taking behaviour, it is likely that their acceptance of risk may be much higher than that of those who specify countermeasures. A study of convicted bank robbers found that nearly 62% of the sample believed their risk of capture prior to their last robbery to have been 'very low' while 17% 'didn't think' about it (Gill, 2004: 91). Some also admitted to wilfully ignoring risk to maintain their morale. Another study, this time of pickpockets, found that:

> … 76 percent of active criminals and 89 percent of the most violent criminals either perceive no risk of apprehension or have no thought about the likely punishments for their crimes.
>
> Anderson, 2002: 295

Although the perceptions of different types of offender may vary considerably, the significance of these findings is heightened by the fact that all were repeat or experienced offenders, so their perceptions were grounded on lived and presumably profitable experience. This presents an important challenge to the notion of an objective or 'actual' risk as opposed to a subjective or

'perceived' risk. It introduces a third, more radical perspective which argues that risk is a wholly cultural construct that derives from the value systems of individuals and groups and the social, political, economic and cultural context that surrounds them.

Social Science and Cultural Theory Perspective

Within the engineering and psychological perspectives, the distinction between objective and perceived risk is accused of presenting the lay-person's view as 'subjective and emotional' (Adams, 2000: 10) even 'neurotic' (Adams, 2000: 13). Even more sympathetic perspectives that acknowledge the importance of risk perception and fear, still maintain that something called 'objective risk' exists:

> Studies such as the European Social Survey, the British Crime Survey, and the International Crime Victim Survey all substantiate the view that across Europe fear of crime is (a) common, and (b) a problem in its own right, separate to crime itself (Hale, 1996; van Kesteren et al., 2000). Not only has fear of crime and disorder emerged as an exigent experience amongst the population of European countries; some researchers have suggested people tend to experience 'fear' beyond the objective risk of any likely victimisation (Hale, 1996; Vanderveen, 2006).
>
> Gray, Jackson and Farrell, 2008: 3

Hence risk is the domain of experts and the risk perceptions of lay people are, at best, distorted versions of reality, rather than a reality of their own. Could this at least partly explain why security risk management in organisations is confined to an isolated department of experts? Adams argues that *everyone* is a risk expert because risk management is an inherent part of daily life and work. This is every bit as true for managers and employees as it is for private individuals, so assessing and understanding their perceptions of security risks provides important insights into their *risk reality*.

In my project, I found that process owners – no matter how junior in the organisational hierarchy – were often well placed to give informed opinions about the specific risks pertaining to their processes, because they work with them every day. This said, they were also capable of overlooking some risks that could appear obvious to an outsider such as myself, and they may be unaware of potential risk consequences for the world outside of their specific process area. Nevertheless, Adams argues that professional 'risk experts' fundamentally misunderstand how people approach risk. This has important implications for risk theory and practice:

> The starting point of any theory of risk must be that everyone willingly takes risks. This is not the starting point of most of the literature on risk.
>
> Adams, 2000: 16

As illustrated earlier with the examples of bank robbers and pickpockets, offenders may be exceptionally willing risk-takers as well as adept at 'blocking out' risk perceptions to enable them to operate with confidence. One of the aims of the security risk manager must be to raise their perception of risk in order to deter them.

The Royal Society revised their report in 1992 and re-titled it *Risk: Analysis, Perception and Management*. The new edition sought to modify the view of its previous document by including in its terms of reference an aim to 'bridge the gap between what is stated to be scientific, and capable of being measured, and the way in which public opinion gauges risks and makes decisions' (Royal Society, 1992: 1). It added two new chapters written by social scientists to explore the aspects of risk that seemed to elude objective measurement. However, as Adams (2000: 9) astutely observes,

the newly added contributions left the identified 'gap' wide open, as they flatly contradict the other chapters' separation of objective and subjective risk 'to the extent that it is no longer a mainstream position' (Royal Society, 1992: 89-90).

So, understanding of risk *perception* evolved from a view that it is a product of individual psychology (i.e. an 'irrational' perception of an objective reality), to one that acknowledges the impact of 'social, cultural and political processes' (Royal Society, 1992: 90) in defining risk as a phenomenon. Hence, 'acceptable risk is .... best characterised as a decision problem, involving values, as well as both agreed-upon and contested facts' (Royal Society, 1992: 92).

The primary challenge to the engineering and psychological positions – which are still held by most government departments and many risk professionals – came in the form of the Cultural Theory of Risk (Douglas, 1982; Schwartz and Thompson, 1990). Devised by anthropologist Mary Douglas as the 'grid-group' model, the theory was originally about social organisation and 'emerged from African ethnography as a way of trying to understand the distribution of ancestor cults, demons and witchcraft' (Douglas, 2006: 6). It was first applied to risk in the 1960s to understand changing attitudes to nuclear power and to explore a sociological alternative to the psychometric theories underpinning the psychological perspective on risk which then dominated the field. It was later adapted for application to other societies and to business organisations, which – as cited earlier with reference to Chester Barnard – are essentially social systems. Douglas reflects:

> What had started as a static mapping of cultures upon organisations was thereby transformed into a dynamic theoretical system. It made a double attack on methodological individualism and philosophical relativism. It put cultural theory into the heart of policy analysis and ethical theory.
>
> Douglas, 2006: 8-9

Cultural Theory presents risk as a construct defined by the cultural orientation and positionality of social groups and individuals. As the Royal Society eventually recognised in their second report:

> Cultural bias is what shapes the risks that groups choose to identify, in ways that cannot be explained by individual psychology or by natural science analysis of 'objective' risks.
>
> Royal Society, 1992: 112

Cultural Theory is most useful to me because it provides a structure – not just for understanding the risks themselves – but also how key actors and groups (managers, employees and, of course, offenders) perceive them.

The model comprises two dimensions. A 'group' scale indicates degrees of individualism versus collectivism:

> The group dimension measures how much of people's lives is controlled by the group they live in. An individual needs to accept constraints on his/her behaviour by the mere fact of belonging to a group. For a group to continue to exist at all there will be some collective pressure to signal loyalty.
>
> Douglas, 2006: 3

People who tend to work alone are plotted as 'low group', while those who are more team oriented are plotted as 'high'. In perpendicular juxtaposition, a 'grid' scale indicates the degree of compliance with (or subjugation to) rule structures. Those who work in highly regulated areas are plotted 'high grid', while those with greater discretion in their decision making go at the bottom. The resulting model produces four quadrants showing 'cultural biases' which are labelled *fatalist,*

hierarchist (or *'positional'), individualist* and *egalitarian* (or '*sectarian'*). Figure 2 summarises the typology with a simplification of the traits:

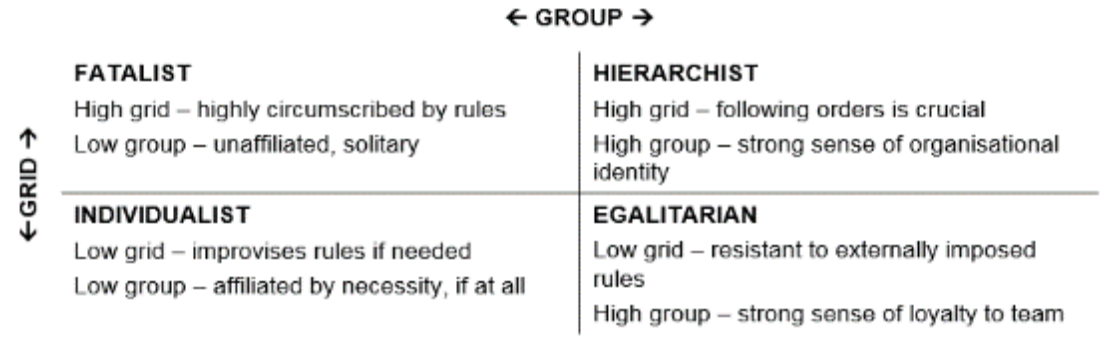


Figure 2: The Cultural Theory of Risk

Mars (1984) applied the model to an anthropological study of workplace offenders, which he classified using a typology based on animal characteristics as shown in Figure 3.

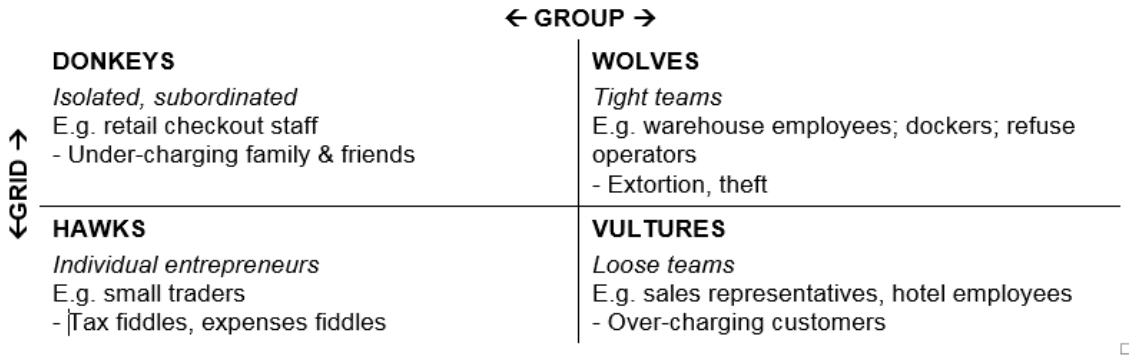


Figure 3: Mars' anthropology of workplace dishonesty

This application of cultural theory provides insights into how offenders manage risks and exploit opportunities, organising themselves in different ways to adapt to the circumstances of their roles. While the organising process may not be planned, it is certainly rational in the context of the offenders' perceptions. Those responsible for managing security risks benefit from this approach because it provides them with a structured insight into offender perspectives. It also encourages them to consider how employees are organised, their workplace culture and the types of formal and informal leadership they follow. It also raises questions about how people are supervised, nurtured, bonded and abandoned to their own devices, and provides a useful counterpoint to criminological theories that emphasise situation and opportunity. Of course, cultural theory can and should also be applied to the organisational culture – particularly that of the leadership –present in workplace scenarios. Weak leadership provides opportunities for strong, natural but perhaps ill-intentioned individuals to occupy the vacuum, so the method is by no means limited to understanding offenders.

To summarise this section on risk, while the 'true nature' of risk is philosophically disputed, my project found that the various perspectives are not irreconcilable in the practical setting. They all agree that risk is about uncertainty and a cultural theory of risk must be able to accept and embrace the cultural perceptions of 'risk experts' alongside those of lay people who, as experts in their own disciplines, possess a different kind of risk awareness.

In my project, working with chemists, engineers and financial specialists required empathy and awareness of the professional cultures of each group and the individuals within them. Designers, marketers, sales people and other creative professions present differing and sometimes conflicting perceptions of risk. However, if unified in a holistic approach, these differences present an opportunity for a more comprehensive assessment of risks as perceived from all the perspectives represented.

As a practitioner trying to solve problems, I found the value of the three perspectives discussed to be primarily in their utility as frameworks for listening to and communicating with people with insight into the security risk environment. At this point in time and in my role, this is infinitely more useful than a concocted, generic definition of risk that stimulates debate rather than action:

> Coming up with a single, clear, unambiguous definition for 'risk' is too hard. Redefining 'risk' in a new way is a bad idea and unhelpful. The best approach is not to define 'risk' in standards at all. There is no need to lay down a strict definition and expect people to agree with it.
>
> Leitch, 2010

But managing risk is not just about coordinating the thoughts and efforts of colleagues. If, as opportunistic theories of crime suggest, security risks are a product of free will and applied ingenuity, then one way to approach the problem is to empathise with the offender and exploit their perception of risk and reward. The psychological view on risk perception is useful because it can provide insights into what may inform individuals' risk perspectives to aid understanding and communication, while the cultural theory provides a framework for understanding group perspectives and other aspects of their social structure and organisation.

The discussion of security risks presents them as a problem which businesses must try to solve. The next section explores what the literature says about how various models of security risk management attempt to do so.

Security Risk Management

Much of what is written on the management of *security* risks is framed within the wider literature of *policing*. This is appropriate because the police, along with the military and intelligence services, do manage those security risks that emerge within their strategic and operational scope. It is likely that most people, especially in developed societies, think of these public entities as the primary response to security threats with exclusive responsibility for the prevention and investigation of crime and other forms of disorder. If this was ever true, it has been in steady decline since the mid-20th century (Reiner, 2000). Certainly, the 'public police' are afforded special powers because they are a manifestation of state control – 'custodians of the state's monopoly of legitimate coercion' (Waddington, 1999: 64). However, they also have significant limitations, such as restrictions on entering private property without a legally defined reason, e.g. a justifiable belief that an offence has occurred or is in progress.

Further, the relatively recent expansion in private control of space for public access, e.g. industrial estates (Johnstone, Leitner, Shapland and Wiles, 1994) and shopping malls (Wakefield, 2000) and the emergence of vast data estates controlled by private companies, such as banks, insurers and social media companies has had a significant impact on the effective capabilities of the public policing form. In response, and fuelled by a wide range of social, political and economic changes,

there was a 'rebirth of *private* policing' (Johnston, 1992, emphasis added) which continues to grow. Analysis by *The Guardian* newspaper indicates the current global size and value of the sector:

> More than 40 countries – including the US, China, Canada, Australia and the UK – have more workers hired to protect specific people, places and things than police officers with a mandate to protect the public at large, according to the data. In Britain, 232,000 private guards were employed in 2015, compared with 151,000 police.
>
> The global market for private security services, which include private guarding, surveillance and armed transport, is now worth an estimated $180bn (£140bn), and is projected to grow to $240bn by 2020.
>
> The Guardian, 12 May 2017

Private policing personnel work in the public sphere as security guards (Shearing and Stenning, 2014) or operating security technology, such as CCTV and detection devices in public space (Wakefield and Button, 2014). They also run private prisons, provide prisoner escort services and even provide investigative services where public provision is inadequate. In my RAL8, I wrote about the impact my previous research has had on this area, which successive British governments have sought to bring under statutory regulation. Leaving to one side the many moral and ethical issues revealed by the various scandals involving private investigators (e.g. the use of their services by journalists which eventually led to the Leveson Enquiry), they demonstrate the power that someone with investigative skills can extract from the availability of technology and access to personal data. It is also true that private investigators work for both the defence and the prosecution in both civil and criminal cases (Gill, Hart and Stevens, 1996; Gill and Hart, 1997, 1997b, 1997c; Livingstone and Hart, 2003) and private security consultants provide expert forensic accounting and computing services to the police and public prosecutors (Gill, M and Hart, J, 1999; Williams, 2014). The availability of such resources in the private sector provides access to a means of achieving justice that would not be available under an absolute state monopoly. Private security companies are even called upon 'to manage issues of national security, including terrorism, climate change and organised crime' (Petersen, 2014: 78) and have played important and sometimes controversial roles in civil and inter-state warfare and post-conflict zones.

Their work in the public domain is usually a product of the state contracting-out services for economic reasons and to preserve public police for situations where their special powers are really needed. Similarly, enabling private policing provision to private customers is justified by the argument that public provision should focus on the protection of the most vulnerable in society, while businesses – who take exceptional risks for exceptional rewards – should attend to their own protection. This is part of a process of 'responsibilization' (Garland, 2001) by which the state seeks greater support from private citizens and organisations to prevent crime but it also empowers the potential victim – including commercial companies – to take action in a form that is consistent with their business interests and values, while remaining within the law. There are also a range of practical considerations that are especially applicable to global multi-national organisations – such as mine – that operate in multiple jurisdictions and a wide range of security risk environments where public provision may be limited or non-existent. As an example, my RAL8 summarised an international security consultancy project that I was involved for a major manufacturer of fast-moving consumer goods (FMCGs). The project sought to understand the dynamics of the illicit international market in such products and the use of public policing resources to carry this out

could never have been justified. Moreover, there are practical and jurisdictional constraints bearing on law enforcement officers in such scenarios that do not apply to private security consultants.

An additional business consideration is that the public police, as designated 'law enforcement agencies', are duty-bound to the criminal justice system and can often only act after a law has been broken. Bringing offenders to justice is important to society, but it doesn't replace the losses or remedy the disruption to victims caused by the offence. Private policing places a far greater emphasis on managing security risks through proactive prevention, i.e. intervention *before* the offence or risk event takes place. Practitioners lack the special legal powers of the public police, but they do have privileged access to the private domains where they are paid to operate. However, to be effective they also need sufficient understanding of business processes and the confidence of process owners – an issue that is integral to the approach produced by my project.

In addition to the private policing forms which are external to organisations, businesses and other organisations – including public sector and not-for-profit entities – also need their own in-house expertise, not least to help manage external provision or to attend to internal matters that may be too sensitive to share with outsiders. This kind of specialist capability is referred to as *corporate security*:

> Corporate security is a discrete portion of this greater security domain with distinct drivers and skills. It is the practicing sector that provides internal security services and functions within either a public or a private enterprise in the protection of valued assets.
>
> Brooks and Corkhill, 2014: 216

Corporate security is an inward looking organisational function, focussing on security risks presented by employees and contractors. It is 'embedded in the organization itself, exploiting as required the other elements of the private security industry' (Brooks and Corkhill, 2014: 218) as well as liaising with the public police, especially when responding to external threats.

Within the academic literature and when 'compared to public policing, private contract security, and national security in criminology, sociology, political science, history, and other disciplines in recent years, corporate security has received little attention' (Walby and Lippert, 2014: 1). Some earlier attempts to explore the niche provide useful insights into how corporate security managers might spend their guarding budgets (George and Button, 1994; Button and George, 1995), but times have moved on and corporate security responsibilities have grown, as have the range and complexity of threats, countermeasures and relationships involved in security risk management. A partial summary of this complexity is summarised in Figure 4 (from Bamfield, 2014: 793):

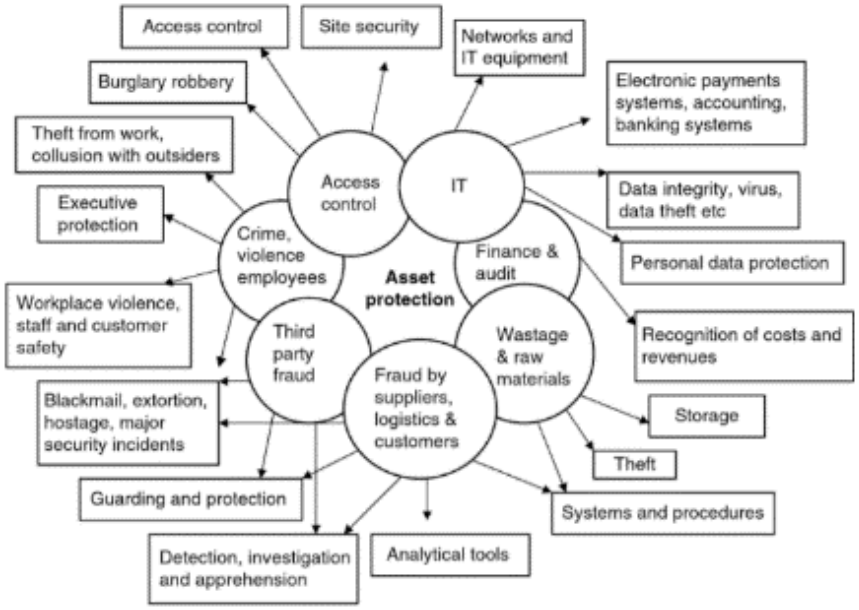


Figure 4: Security issues in a business organisation

Security risks can have many consequences for businesses, ranging from minor disruptions to a total loss of functionality and ultimate annihilation. How their internal response has evolved over time is interesting and important because it suggests a trajectory that could indicate the future direction of the discipline.

Studies have found that the way corporate security departments operate is influenced by the practitioners' former careers (Shearing and Stenning, 1983; Manunta, 1998; Gill, 2014). It has been observed that 'an aspect of professionalism in the corporate security domain is shared backgrounds, such as those of ex-military and law enforcement professionals' (Brooks and Corkill, 2014: 220). Indeed, there is a widespread migration of expertise from the public sector to all forms of private policing: what Hoogenboom (1991) calls the 'blue drain' (although a 'green drain' of former military personnel also exists).

The earliest manifestation of a corporate security function is referred to figuratively and literally as the 'works police' (Button, 2016: 56). In the UK, this comprised primarily uniformed officers conducting patrols and inspections on industrial sites, occasionally searching vehicles or personnel, but primarily facing outwards to the world beyond the perimeter fence. Although some were members of the main workforce who were unable to continue with their normal duties due to injury, most would have military experience from conscription and would be accustomed to discipline and wearing a uniform.

Some observers have commented that former military personnel instinctively regard the facilities they protect as a 'defensive position' to be fortified against attack and security scholar Giovanni Manunta (himself a former paratrooper) formulated a set of security stereotypes based on chess board pieces in which he likens the ex-military practitioner as the *rook* (Manunta, 1998). Although imbued with the strength of a castle rampart and the speed to traverse the board in one move, the rook is confined to the outside of the business and has difficulty negotiating complex obstacles. In addition, commercial spaces are not usually fortresses and many seek to be open and inviting and provide a managed welcome to both insiders and outsiders.

Corporate security evolved with the introduction of the *loss prevention* concept. Kletz (1999) suggests that this terminology emerged mid-20th century from a new emphasis on safety management in industry, intended to tackle an increase in safety incidents consequent to new and more dangerous technologies. It started to be applied to the management of security during the 1970s, when those responsible for security functions started to consider the economic contribution of their work in preventing the financial consequences of security incidents (Rogers, 2016). An additional explanation may be related to aesthetics and the need to appear more business-friendly, as some contemporary observers suggested that even the term security 'carries a stigma':

> ... the very word suggests police, badges, alarms, thieves, burglars, and some generally negative and even repellent mental images
>
> Astor, 1978, cited by Purpura, 2013: 7

This said, 'loss prevention' can turn out to be more about 'loss detection' and the ensuing reactive investigations that are required *after* incidents occur. When protective measures fail and investigative responses are needed, security practitioners are expected to have policing skills, particularly those of the detective. In developing his chess game, Manunta dubs the ex-police security practitioner a 'knight' who rides out to fight crime and deliver justice. He or she can cut corners and jump over other pieces, but has limited reach and can often only achieve the desired destination after several moves, by which time the game may have changed beyond recognition. As mentioned in my introduction, many non-security managers have a cultural expectation that security practitioners are solely concerned with the detection of offenders. However, commercial organisations are not law enforcement agencies and focussing on the offender at the expense of the system that allowed them to offend can leave it exposed to repeat victimisation.

In some organisations, the 'loss prevention department' developed into a broader-based, more comprehensive entity to incorporate safety, auditing and other professional functions. Its purpose was to reduce all forms of loss, not just those resulting from criminal behaviour, while presenting a positive outlook that was consistent with the values of the business.

Another important terminology to emerge around the same period is the term *asset protection*, adopted by security departments 'to be recognised for their contribution to protecting assets and people' (Dalton, 2003: 22). This is a useful term that accommodates the broadening definition of what organisations identify as 'assets'. While the early days of industry focussed more on physical property and people, the emergence of the Digital Age has placed greater emphasis on intangible assets. These include data and specific types of knowledge, as well as more elusive yet critically important concepts, such as brand reputation.

A further extension of the loss prevention and asset protection concepts emerges in the form of *enterprise risk management*. Wakefield (2014) explains the implications for the sorts of knowledge, understanding and insight this widening field demands:

> As corporations shift toward more holistic approaches to risk management, heads of corporate security must demonstrate that they can effectively engage with these. This requires them to be able to communicate a thorough understanding of the wider business, and show the contribution that security can make to risk-taking and risk reduction as a way of adding value to the organization.
>
> Wakefield, 2014: 235

It is significant that Wakefield writes of security managers 'engaging' with other forms of risk management, rather than managing them. Some companies turn to professional managers from other disciplines to manage security within a broader portfolio. Manunta's third chess-piece stereotype is the 'bishop': the non-security professional, usually with an administrative, legal or financial background. This is the case in my company, wherein corporate security function reports to the most senior legal counsel. Unencumbered by the professional assumptions and 'baggage' of the rook and the knight, the bishop is commercially and politically savvy, knows the business and is well connected (as it sits next to the most powerful pieces on the board). The bishop moves diagonally across the columns and rows of the board (i.e. organisation), but may lack the technical or subject matter expertise needed and must therefore import that knowledge by building a specialist team – often comprising a variety of 'rooks' and 'knights'. One of the primary challenges pertaining not just to the bishop but to all non-security specialist managers is ensuring they have enough security knowledge to make informed decisions based on the advice inputs security specialists provide them.

Of course, these various forms of expertise, skills and orientation can be blended, and many former military and police personnel have an excellent grasp of the business mission, as well as first-rate management and organisational skills. The importance of the right combination of technical and business knowledge was confirmed by recent research which found that corporate security personnel consider it very important that 'the head of security is recognised for both security and business knowledge' (Gill and Randall, 2014: 65) and that 'excellent corporate security was about embracing business' (Gill and Randall, 2014: 73).

Organisations attend to internal security risk management by incorporating various forms of specialist knowledge within their structures, usually embedded within a dedicated department. However, my project brought me to the view that effectiveness is only really achievable by integrating security risk management into the competence and responsibilities of all managers.

Indeed, the ISO31000:2009 Risk Management standard mentioned briefly in the earlier section on Risk offers a recognised standard that has sought to help organisations 'integrate risk management into [their] overall management system' (ISO, 2009a, p. 9). This is an attractive proposition, but the standard's imperfections have been noted:

> Although the ISO 31000 standard has effectively integrated the principles and practices considered most effective by many experts and researchers in the field, the experience feedback from examples of organizational crises in various sectors should lead managers to question *how* they will integrate it in their organizational strategy.
>
> Lalonde and Boiral, 2012: 272 (emphasis added)

The word 'how' in the above quote is fundamental to my project, because the 2009 standard said little about the various responsibilities of non-risk professionals. A more recent version of the standard (ISO 31000:2018), recognises that it 'remains a challenge for risk professionals to demonstrate the value of making resources available for risk management' (Institute of Risk Management, 2018: 4). This revision:

> …provides more strategic guidance than ISO 31000:2009 and places more emphasis on both the involvement of senior management and the integration of risk management into the organization. This includes the recommendation to develop a statement or policy that confirms a commitment to risk

> management, assigning authority, responsibility and accountability at the appropriate levels within the organization and ensuring that the necessary resources are allocated to managing risk.
>
> International Organization for Standardization, 2018: 2

Yet this revision did not exist when I conducted my project and it does not recommend integration of risk management knowledge into the skillsets of all managers, nor does it appear to require the process-level depth of penetration of my approach and the enhancement and refinement of management perceptions of risk. The discussion in the previous section presented a view that the nature and extent of risk may be contingent on the perceptions of people so if risks are not perceived, what is there to manage?

Writing in the midst of the Second World War, Maslow (1943) observes:

> [T]he need for safety is seen as an active and dominant mobilizer of the organism's resources only in emergencies, e.g., war, disease, natural catastrophes, crime waves, societal disorganization, neurosis, brain injury, chronically bad situations.
>
> Maslow, 1943: 379

To replace this position with a more proactive and preventive approach – hopefully resulting in the avoidance of adverse events, or at least minimising their probability and impact – it is necessary to actively identify risks. Adopting the principles of opportunistic theories of crime and role-play method, risk identification and assessment requires managers to adopt the positionality of the motivated offender and 'think criminal'.

Specifically addressing the *security* risk management niche, the respected US-based professional security association ASIS International offers a 'guideline' document. *The General Security Risk Assessment Guideline* (ASIS: 2003) brings together a diversity of practical and theoretical expertise on this emerging discipline, while recognising its inherently contingent nature. It acknowledges the need to 'understand the organisation and identify the people and assets at risk' (ASIS, 2003: 6) but says little or nothing about *business process*, other than reference to 'the primary business or endeavour of an enterprise, including its reputation and goodwill' (*ibid*). While this reference to core function is crucial, my approach reaches deeper as it involves the risk assessment of *individual* processes within the business as a system.

In addition, the ASIS Guideline acknowledges the value of both quantitative and qualitative approaches to risk assessment, yet its *Recommended Practice Advisory* relies extensively on reactive data generated by 'a history of such events' (ASIS, 2003: 6) and defines the 'probability of loss risk as a concept based upon considerations of such issues as prior incidents, trends, warnings, or threats, and such events occurring at the enterprise' (ASIS, 2003: 6). It does acknowledge that risk can be a product of 'circumstances in the local environment' (*ibid.*) which could be interpreted to refer to criminogenic characteristics, such as opportunities to crime that have not yet been exploited. However, the main emphasis is on data from previous incidents. Interpreted harshly, this could suggest that success can only be informed by prior failure, but this is unfair in many settings. The emphasis on frequency of occurrence may be appropriate, if events are known to occur frequently. However, this is not the case in my organisation either because incidents are not reported or because the types of incident that do occur tend to be of low frequency but potentially much higher impact.

My approach differs significantly in several ways. First, its emphasis on the significance of *opportunity* distances it from the traditional emphasis on data generated by past incidents and the notion that they are necessarily an indication of future risks. Of course, I would take account of any such data that was available and recommend an appropriate response – particularly if the risks remained untreated. However, I strongly believe that managers must also look for hidden vulnerabilities that have yet to be exploited. My project aims to provide a means of putting the asset protector on the proactive front foot against the attacker, who must recognise that his or her plans are predictable and vulnerable to defeat.

Second, my approach *demands* input and insight from technical and business specialists. This is not simply a matter of inclusiveness – it relies on the deep insights that such perspectives can provide to a security risk professional who understands how little he or she knows about the business or business processes under scrutiny. As discussed earlier, this also provides a means of enhancing the knowledge and perceptions of security risks by managers who are not trained in security risk management.

For the remainder of this section, I want to introduce some key management tools that I used in my project and which provide a good indication of how this can be achieved. Management is about achieving organisational synergy, yet the subject of management is vast and full of competing philosophies and models. As early as 1961, Harold Koontz described what he called the 'Management Theory Jungle', successfully capturing the character of the emerging body of management knowledge as grounded in the experiential and field-based observations of its pioneers, yet entangled in the semantics and assumptions of the many disciplines that had followed them. The jungle continues to expand and it would be impossible to cover all the relevant aspects in this thesis. However, the three management concepts that I will refer to in my analysis of findings are *systems theory*, *quality management* and *the McKinsey 7-S framework.*

Systems theory

Developed by Ludwig von Bertalanffy in the 1920s, General Systems Theory views the natural and social world) as a series of systems to be understood holistically, rather than as a sum of their individual components. This rejects the reductionism of other approaches that seek 'to resolve and reduce complex phenomena into elementary parts and processes' (Bertalanffy, 1972: 408-409) and argues that ignoring the 'coordination of parts and processes' (Bertalanffy, 1928: 8) obscures a view of systems as 'organised entities' (Bertalanffy, 1972: 410) in their own right. As Skyttner summarises:

> ... what we need to understand is not the behaviour of individual parts but rather their orchestration. Often, our goal must not be to understand what things are made of, but rather how they are compounded and work together in integrated wholes
>
> Skyttner, 2005: v

Yet the reductionist and holistic perspectives of organisations as systems are not irreconcilable. Most traditional approaches to security tend towards a multi-layered approach to protect the whole. A factory enclosed by a wall and perhaps a perimeter fence is a good example of a system being protected from external threats using a 'defence-in-depth' approach to 'deter, delay or detect' anyone contemplating illicit access. However, this does not treat internal threats from those who

have been granted legitimate access, such as employees, contractors and customers. A more granular approach that allows each system component or process to benefit from security risk assessment is needed. At the same time, as *systems engineering* 'is distinguished by its practical philosophy that advocates holism in cognition and in decision-making' (Haimes, 2015: 5), each process must be assessed in terms of its contribution to the whole. My approach shifts between the two perspectives, zooming in and out of areas of interest as they arise.

Systems are also about people and how they relate to each other and the tasks they perform. Socio-technical systems theory emerged in the aftermath of World War II with the work of the Tavistock Institute's exploration of 'group relations in depth at all levels' (Trist,1981: 7) and expands systems theory to view the organisation as 'a combination of social and technical parts ... that it is open to its environment' (Appelbaum, 1997: 453).

> The concept of the socio-technical system was established to stress the reciprocal interrelationship between humans and machines and to foster the programme of shaping both the technical and the social conditions of work, in such a way that efficiency and humanity would not contradict each other any longer.
>
> Ropohl, 1999: 186

My approach therefore adopts a 'systems view' (Arbnor and Bjerke, 2009: 103) of organisations and business activities by seeking to understand the combined technical and human contribution to the security of systems at both the process and holistic levels. Applying this view using multi-disciplinary teams to combine security and business expertise helps to embed security risk management within the wider management of the organisation and 'should provide a way to bridge the gaps and remove some of the barriers that exist between the various disciplines' (Haimes, 2015: 15).

Quality management

Quality is 'an outcome – a characteristic of a product or service provided to a customer, and the hallmark of an organisation which has satisfied all of its stakeholders' (Charter Quality Institute, 2015). In addition to other harms they may cause, security incidents have an adverse effect on quality because they cause waste, whether in terms of materials, effort or lost opportunities. Quality management seeks to improve productivity and performance by eliminating waste and comprises the series of activities, functions and disciplines that enable an organisation to deliver quality and achieve conformance to requirements.

In my MSc dissertation (Hart, 1993), I argued that security is an attribute of quality because its absence causes defects and other forms of non-conformance to specifications that must be paid for – either by the producer or by the consumer. An obvious example is provided by the direct cost of retail crime, which in the UK in 2013 was £511 million – while a less obvious one may be cybercrime – estimated in the same year to cost up to US$100 billion in the US alone. The impact of these losses is felt and funded to varying degrees by all stakeholders, including tax-paying consumers. However, proponents of quality management argue that this need not be so:

> All non-conformances are caused ... Anything that is caused can be prevented.
>
> Crosby, 1984: 7

Integrating security risk management into the cycle of continuous improvement demanded by quality management, provides a tangible means of bringing security into the mainstream, as well as a real opportunity to improve quality – which benefits us all.

Earlier, I wrote of the need to broaden our understanding of system inputs and outputs to include aspects of security risk management. This needs to be broadened further to incorporate every aspect of organisation, which moves us on to the McKinsey 7-S framework.

McKinsey 7-S framework

The McKinsey 7-S framework is a form of systems view that considers 'hard' and 'soft' aspects of organisations and was specifically formulated as 'a new framework for organisational thought' (Waterman, Peters and Phillips, 1980: 17). Dissatisfied with the limitations of the contemporary obsession with restructuring as the only pathway to achieving positive change, its creators set about finding a more complete set of aspects or dimensions of organisation and produced a list of headings that are presented in Figure 5 in a web of interdependency.

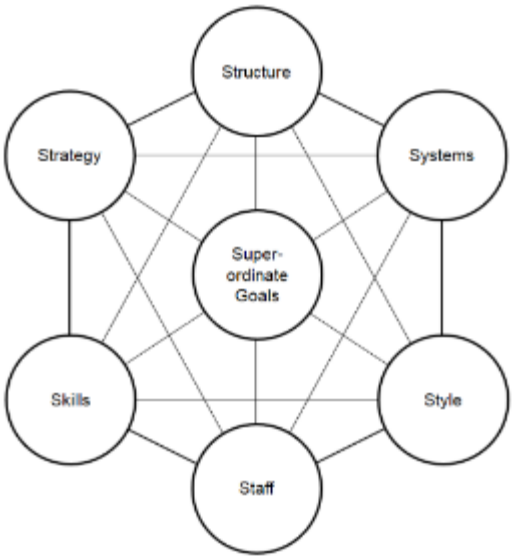


Figure 5: The McKinsey 7-S Model

The 7-S has proved to be an enduring model, although it has been subject to criticism – not least because it was used to define some companies as examples of business excellence that later failed. As a prescriptive tool for organisational design with its emphasis on the importance of achieving the right 'fit' between the different elements, it may seem to propose a stability or even immobility that can turn into obsolescence:

> Fit implies a sense of permanence. It is concerned with maintaining a steady state rather than guiding the constant evolution of new advantages. It is also very predictable, making the company an easy target for competitors. If the organization is so tightly galvanized around a single objective, it can tend to make a firm less flexible and unable to change strategy or the rest of the 7-S's to meet new needs.
>
> D'aveni, 1994:30

However, in my project, this tool has proved eminently useful as an 'agenda of considerations' to identify the organisational factors contributing to the causality of security risks and security incidents. It has also provided a structure for communicating security analyses in a meaningful way to general and specialist managers who may not normally consider security in their thinking. To illustrate with an example using organisational structure, a traditional, top-down hierarchy can

impede employees' ability and preparedness to respond to adverse events. Aoki (1986) notes that, in horizontal structures 'workers are gradually made familiar with the whole work process and become capable of coping with unexpected emergencies' gaining them a 'grass roots capability to cope with emergent events fostered by collective learning by doing (Aoki, 1986: 972). In contrast, within vertical or hierarchical structures

> … management has a priori knowledge of the overall production technology. But their capacity to identify emergent events affecting production technology of subunits and to enforce the implementation of appropriate operational decisions upon said subunits may be limited and costly, simply because management is removed from operational activities.
>
> Aoki, 1986: 975

Similarly, skills deficits, flawed or absent strategies, inappropriate choice of staff, poor management style or inconsistency with shared values and organisational goals – can contribute to vulnerabilities that offenders can identify and exploit. The 7-S provides any organisation with a way of knowing itself better and holistically seeking out its vulnerabilities and exposures.

Summary

In summary, this chapter has presented the three main cornerstones that form the basis of my theoretical framework. Security as a form of applied criminology provides a wealth of material to ask and answer questions in the field about what opportunities to breach security are present and why an offender might be motivated to exploit them, as well as the criminogenic characteristics of physical or procedural situations where such opportunities arise.

Risk theory explores objective and subjective perspectives on risk and provides additional insights into offender perceptions, as well as those of process owners and those decision-makers who are closest to the situations where risks may emerge. It also provides a vital cornerstone to the concept of security risk management, as it requires preventive efforts to be targeted to where they are most needed.

Security risk management is the organisational response to the threat of intentional harm. Usually delegated from mainstream management as a specialism, it is presented as a discipline that requires understanding and awareness of security risks and specialist knowledge of techniques and technology to reduce them. It also requires understanding of the characteristics of the organisation, its business processes and how they are managed.

Taken overall, I believe the literature suggests that the current configuration of the security risk management function as a separate department, isolated from core business activities, only makes sense regarding its investigative or reactive role. A centre of technical expertise offering advice or specifications on security measures is a useful asset, but a truly proactive approach to managing security risks requires a deeper penetration into the systems by which business is delivered so that this important discipline becomes embedded within business processes. While there is a need to equip managers and employees with security skills and knowledge, it is they are who are in the best position to identify and assess risks at their level, and to communicate them to more strategic decision-makers who can assess the data in the context of the wider organisation.

The next chapter presents my project methodology and how I arrived at a practical approach to work towards these goals by trial and error in the field.

CHAPTER 5: METHODOLOGY

This chapter is about how I conducted my research and the underlying principles of knowledge development that I engaged with while developing my approach. I have structured the chapter as a narrative account of my methodological journey through the two project stages because I believe this provides the most honest and accurate account of the work I did.

In the interests of clarity, the term 'method' refers to the research methods I employed to gather and analyse my data, while the term 'approach' (except in 'methodological approach') refers to the set of tools and techniques that my project produced.

FAMDoc

This first stage of my project sought to address the security risks pertaining to my company's certificates and reports, how these documents are vulnerable to falsification, adulteration and misuse (FAMDoc) and the reputational significance of this exposure. My DPS4561 submission proposed that I would research this problem and attempt to implement and evaluate a solution to better protect the documents' authenticity.

I perceived the problem (and, if I'm honest, its likely solution) as amenable to rational forms of empirical research that incorporated both quantitative and qualitative methods to be combined 'as complementary to each other' (Layder, 1993: 109). My methodological approach was firmly rooted in an empiricist ontology derived from the 'method of science' (Burns, 2000: 5, citing Kerlinger, 1986) and maintained 'the positivist notion of a singular reality, the one and only truth that is out there waiting to be discovered by objective and value-free inquiry' (Feilzer, 2010: 6).

Indeed, it was consistent with the engineering and psychological perspectives on risk discussed in the previous chapter. Reflecting on it now, I recognise that I believed that any risks my research would identify existed in an objective reality that I, as a security risk expert, could reveal to others and thereby correct any 'erroneous' perceptions of risk they may have formed, as well as offering some explanation as to why they were mistaken. I also believed that these risks could be managed, reduced or even eliminated with carefully crafted interventions based on the expert knowledge of myself and others.

Research methods

I selected my research methods for the FAMDoc project accordingly, using a multi-layered approach to achieve triangulation between background research, a survey, interviews and group work, followed by some observational studies. The background research would identify how the problem manifested itself as such and give an indication of the questions I needed to ask. The survey would provide me with general 'lay of the land' data about the size and broad shape of the problem and existing practices within the business. The interviews and group work would provide me with an opportunity to gain a more granular insight to how people work and think, while the observations would allow me to identify nuance as well as confirm or rebut what people said compared or contrasted to what they do.

I had relied on variations of this methodological approach in numerous previous research projects (e.g. Gill and Hart, 1996, 1997a, 1997b, 1997c, 1999; Gill, Hart and Livingstone, 2000; Livingstone

and Hart, 2003), was well-versed and comfortable in using it, and believed it to provide a sound balance between macro- and micro-level views of reality. Put simply, I chose it because I believed it would take me to something that I could accept, embrace and present to others as credible (and publishable) 'truth'.

Background research

So, I started FAMDoc by conducting a documentary analysis of the available reports or complaints which revealed the types of attack our documents seemed to attract. Drawing from my knowledge of offender motivation and criminology, this allowed me to formulate ideas *a priori* about why these documents were a target and how perpetrators might respond to existing deterrents or countermeasures. Also taking account of verbal input from colleagues who shared their knowledge and experience, my analysis produced a typology of attack types, resulting in the project acronym (*Falsification, Adulteration and Misuse of Documentation*).

Self-completion questionnaire

I needed to discover how these documents were produced and used in business as well as users' awareness and experience of the three attack types. My next step was therefore to design a survey in the form of a simple self-completion questionnaire 'to give a sense of the whole body of data from which … examples are drawn' (Layder, 1993: 111). My line manager advised me to keep the questionnaire short because respondents would probably ignore anything too detailed, so I designed it with a combination of closed and open items to allow them to add more granular detail if they wished, but without obligation. After piloting on two Affiliates who I then excluded from the final survey, I emailed the questionnaire to every remaining Affiliate and received 51 returns, representing a response rate of around 34% (N=148). However, there were many problems with the way respondents had completed the questionnaire, which I will discuss in the next chapter.

Observational studies

The questionnaire was to be followed by some observational studies, semi-structured interviews and group work in a sample of company locations. The sample selection of locations was based on a range of rational factors that I agreed with my line management and business leaders to be salient. These included ensuring representation of a cross-section of small, medium and large Affiliates, whether there had been previous reports of document tampering, representation of all company-defined geographical regions, and the responses to the self-completion questionnaire. Consideration of these factors produced a range of hypothetical explanations including 'smaller Affiliates may be less strict about applying procedures', 'larger Affiliates produce more volume and may be more prone to error', along with other suggestions from colleagues about possible cause.

I managed to conduct various observational studies during this stage of the research, but the sampling framework was severely disrupted by operational requirements. Again, I will explain these disruptions in more detail in the next chapter.

FAMDoc outcomes

When I eventually completed the data gathering process as best I could, I worked with a colleague from the Global IT Department on a technical solution in the form of a smartphone app to read a new secure QR code which we proposed to add to all hard copy certificates and reports. The code

– unique to the company and unreadable by other apps – would display key data on the device that could be compared with the information on the hard copy. If they didn't match, the document should not be accepted and there was a facility to report it immediately. We submitted our idea to a special 'Innovations' unit within the company that was recently set up to process employee ideas for performance enhancements and new business ideas. The proposal was accepted in principle, but had to take its place in a queue along with other ideas. This obstacle was unforeseen and did not exist when I began the project. It was therefore the cause of some anxiety because my original project plan included activities pertaining to the solution *after* its implementation. At best, this would cause a significant delay but at worst, it would disrupt my entire project plan.

In summary, my original proposal was for a neat, orderly and conventional approach to a defined problem (FAMDoc). Its intended focus was to be the *solution* to that problem, rather than the means and process of understanding and trying to solve it. However, in response to shifting priorities within my company, but also as a product of what I had learnt and developed up until that point, my project evolved into a second stage and a significant expansion of the original scope. Although it wasn't intended, the transition was a logical and eventually welcome progression.

BPSA

This second stage – dubbed *Business Process Security Analysis* (BPSA) – addressed a broader range of problems and delved much deeper into the company's approach to designing and securing its business activities. It also incorporated a shift in focus to the *process* of developing solutions, rather than the solutions or other outcomes themselves. Hence, while FAMDoc was intended to provide an *example* of how security risk management could be integrated into mainstream management practice, BPSA presents at least the beginning of a practical means of achieving that integration.

However, in methodological terms, the disruptions and changes of priority that I had experienced during the earlier stage of my project had taken me to unfamiliar research terrain. This challenged my trusted ontology and I confess to entertaining thoughts that I had made a massive mistake in my choice of topic. This is a lonely place to reside, but others had been there before:

> The extraordinary complexity of organizations, at multiple levels of analysis, presents researchers with tough conceptual and methodological barriers. Unfortunately ... the response has frequently been one of ignoring away the messy concepts and the soft issues, of studying the outcomes but not the processes, and of nomothetically treating firms as black boxes.
>
> Parkhe, 1993: 246

The FAMDoc experience demonstrated that the shifting characteristics and priorities of the business environment were proving not to be amenable to traditional, monological approaches. My assumptions about a single truth or reality were fading and being replaced by a disorderly collage of multiple realities:

> The single epistemological ideal of a neutral "view from nowhere" has been replaced by multiple views, with each situated somewhere. The research process can no longer be characterised as an 'objective' investigation of the natural (or social) world, or as a cool and reductionist interrogation of arbitrarily defined 'others'. Instead it has become a dialogic process, an intense (and perhaps endless) 'conversation' between research actors and research subjects ...
>
> Nowotny, Scott and Gibbons, 2003: 4

Attempting to construct this new stage of my project in a linear way would have been trying to make the problem fit the solution and would have produced an output lacking both utility and validity because it wouldn't capture the complexity that confronted me. Tsang observes that '[i]nternational business research has been dominated by quantitative methods, in particular questionnaire surveys' (Tsang, 2013: 195). Such methods only address the problems that are amenable to them, but the evolution of the project from FAMDoc to BPSA demanded a change in methodological approach because the 'dynamic, complex and multidimensional' (Tsang, 2013: 195) workplace research environment was proving resistant to the orderly data gathering process previously conceived.

Bricolage

There was no 'perfect fit' between problem and method so I had to 'satisfice' (Simon, 1956: 1) and resort to heuristic problem solving to find workable solutions:

> Heuristics are frugal—that is, they ignore part of the information. Unlike statistical optimization procedures, heuristics do not try to optimize (i.e., find the best solution), but rather satisfice (i.e., find a good-enough solution).
>
> Gigerenzer, 2008: 20

I had to find ways, not just of overcoming the turmoil, but also of *embracing* it as part of the problem I was trying to solve. This required improvisation, so I resorted to *bricolage* as a means of negotiating the problems I encountered. Bricolage provides a theoretical framework for situations that demand improvisation:

> The etymological foundation of bricolage comes from a traditional French expression which denotes crafts-people who creatively use materials left over from other projects to construct new artefacts. To fashion their bricolage projects, bricoleurs use only the tools and materials "at-hand" (Levi-Strauss, 1966). This mode of construction is in direct contrast to the work of engineers, who follow set procedures and have a list of specific tools to carry out their work.
>
> Rogers, 2012: 1

Bricolage 'exists out of respect for the complexity of the lived world' (Kincheloe, 2004: 2) and provides workplace researchers like myself with a means of *cooperating* with the phenomena we are trying to understand. In circumstances where it is impossible to apply scientifically consistent methods, the bricolage makes 'creative use of existing resources [providing] a capacity to mobilize practical knowledge in a way that challenges general theoretical approaches that specify *a priori* how resources should be utilized' (Baker, 2003 cited by Duymedjian and Rüling, 2010: 135).

What bricolage does *not* do is provide a set of methods or tools that have been specifically designed for use in problematic situations. Rather:

> In its hard labours in the domain of complexity the bricolage views research methods actively rather than passively, meaning that we actively construct our research methods from the tools at hand rather than passively receiving the 'correct', universally applicable methodologies.
>
> Kincheloe, 2004: 2

This said, I found bricolage to provide a means of coping and improvising in situations where the world is uncertain:

> Bricolage has been used to characterize organizational practices related to innovation, and several authors relate bricolage to improvisation. Improvisation consists of assembling elements based on simple rules in order to yield an original composition. This mode of action is characterized by a

> coincidence of conception and realization that makes it difficult to clearly distinguish moments of reflection from instances of action. This integration of thought and action allows for a rapid degree of adaptation, which equips organizations to relate better to a turbulent environment.
>
> Duymedjian and Rüling, 2010: 133

The approach ran counter to all my previous learning and flatly challenges the orthodoxy to which I earlier subscribed, but its resonance with the research reality I found myself working in was profound:

> The subversive bricolage accepts that human experience is marked by uncertainties and that order is not always easily established. 'Order in the court' has little authority when the monological judge is resting in his quarters. Indeed, the rationalistic and reductionistic quest for order refuses in its arrogance to listen to the cacophony of lived experience, the coexistence of diverse meanings and interpretations.
>
> Kincheloe, 2004: 5

To move forwards, I had to find ways of gathering data that were intellectually defensible yet flexible and adaptable. The problem was messy, so making sense of it demanded an agile and effective approach that could be responsive to the bear pit of real world commercial organisations while allowing the possibility of data abstraction. My use of bricolage throughout the project took me on a methodological journey that led me to question then change fundamentally the way I think and work. The following sub-sections present the range of methodological approaches I made use of.

Phenomenology-based ethnography

Seeking explanations for decisions and actions 'grounded in the meaning structure of those studied' (Aspers, 2004: 2) and those who guided me, I started to explore phenomenological and interpretivist perspectives that challenge philosophical rationalism and seek to recognise, identify and understand the subjective views and experiences of human beings that natural sciences do not address in the same way. The views and experiences I was particularly interested in were the managers and other employees who I wanted to embrace security risk management as part of their general competence. The perspectives I explored combine disciplines concerned with the understanding of meaning and experience and crucially reject positivist assertions. As a form of 'phenomenology-based ethnography', my approach was about involvement:

> … and "doing it yourself," which generates data derived from immediate experience that can contribute to the reconstruction of the internal viewpoint by uncovering the essence of a phenomenon.
>
> Pfadenhauer and Grenz, 2015: 599

My project required me to develop my role as actor-observer, 'immersed in local situations generating contextually embedded knowledge which emerges from experience' (Coghlan and Brannick (2014): 4). Both my job and my academic engagement required me to act and observe, but in different ways. The process required me to identify and reflect, not only on my own knowledge and perceptions, but also those of others. These included the people I was observing, as well as those who helped me observe by sharing their specialist skills and knowledge. I had to learn to see things from their perspective, as:

> ... an observer of cultural life can understand the data observed only if taken with the "humanistic coefficient", only if he does not limit his observation to his own direct experience of the data but reconstructs the experience and the data in the social context of the people involved.
>
> Znaniecki, 1940: 5

Pietersma characterises this as an empathic process, whereby 'the phenomenological theorist describes or articulates cognitive experience of the standpoint of the cognizer, thinking of as though it were her own, imagining it as if she herself actually had it' (Pietersma, 2000: 8). However, he goes on to insist that:

> As an actual person, the phenomenologist, of course, has her own convictions about what exists or does not, but her phenomenological approach demands that they should not play a role in the way she describes the cognitive experience under discussion.
>
> Pietersma, 2000: 8

However – at least in my case – the *participant* observer must participate.

Role play

Although I shifted between the two roles, I had my own job to do with an explicit mission to intervene in certain situations. As I did not conceal my security and investigative roles, my research subjects would have been fully aware of these responsibilities and this may have had various effects on the quality and flow of information.

In addition, I had to empathise with the offender too, but seeking out opportunities that are attractive to criminals requires a kind of internal role-play, in which the observer 'thinks criminal' and consciously looks for vulnerabilities, lapses in procedure or any design failure that could facilitate an attack. Role-play is a recognised research method that provides 'insight into the dynamics of interpersonal interactions in relationships which cannot be gained from other methods' (O'Sullivan, 2018: 609):

> Role-play is concerned with representing and exploring different people's points of view, and different points of view forge different types of knowledge. It places participants at the centre of the learning experience, and allows them to build their own bridges of understanding. As a result of this informed consideration, they are better able to resolve problems and issues.
>
> O'Sullivan, 2018: 611

It is used extensively in business, for example in so-called 'mystery shopper' exercises, which are very common in the hospitality industry to learn about the customer experience. I have used it most frequently in 'penetration test' exercises, which involve gaining unauthorised access to premises or other resources, to test their security arrangements. The method needs to be used with care for various ethical reasons if others are to be involved, but my use of it remains internal to myself as a means of self-consciously generating an alternative view of the perceived environment.

Process mapping

The significance of the perceptions of actors does not undermine an important premise of this enterprise-based research, which is that an organisation is a system that is responsive to the complexity of its internal and external ecology. Within my company, each national Affiliate and business department presents its own sub-ecology within the corporate whole. These in turn comprise individuals and groups of professionals from a range of disciplines, each with their own ontological and epistemological perspectives. My interactions with individuals and groups in joint observational studies, focus groups, case analyses and other activities continued to establish how systems and their ecologies functioned and the risks they attracted or generated. The elicitation

process produced a range of process maps as diagrammatic representations of 'problem realisations'.

Process mapping provided an invaluable 'orderly' dimension to the work. Drawing from the systems theories introduced in the Literature Review, the technique involves visualising a business, project or facility as a *system* comprising multiple *processes*, each adding cumulative value to a product or service. The process map is a flow chart that provides a view of how each system works and which processes are involved. Processes may operate in series or in parallel, but each must have a clear purpose that should be understood by managers, supervisors and operatives. Processes may also be clustered together, allowing us to view the system in varying degrees of granularity. It isn't always necessary to view systems and processes in minute detail, but having a closer look can sometimes reveal hidden problems that provide opportunities for continuous improvement. Some processes may be performed by a single employee or piece of equipment, while others are more complex and use multiple assets. Assets can be identified in the process map and should be considered as possible targets in the risk assessment, as well as the processes themselves.

I had first used this technique professionally in my very first piece of published research, which was about how the UK police cope with high volume but low impact criminality (Gill, Hart, Livingstone and Stevens, 1996). A fragment for illustration purposes is shown in Figure 6:

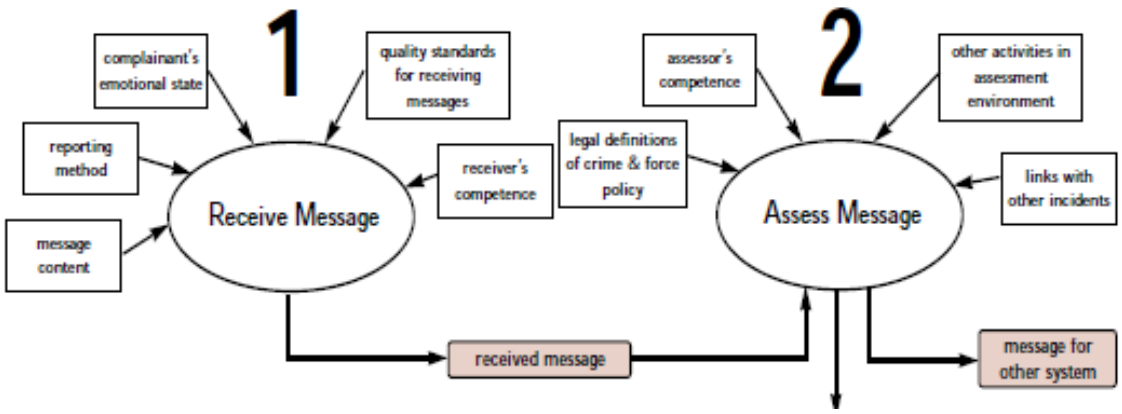


Figure 6: My first professional use of the systems approach

The diagram shows a range of inputs to each process. Processes generate one or more outputs that become inputs into subsequent processes. Using the principles of quality management, it is possible to identify the impact a flawed input to one process might have to the proper operation of all subsequent processes. This applies as much to 'soft' inputs, such as human emotional conditions as it does to 'hard', such as written policy statements and legal definitions. While the component (input, process, output) parts are studied in detail, it is their impact on the behaviour and performance of the whole system that must be understood.

In addition, it was a simple step to apply the method to explore what happens before and after a defined system starts or ends. In FAMDoc, my consultations with employees expanded the scope from a small nucleus of documented processes that specified how security paper was to be stored, issued, used and transmitted, to include other systems that generated the data to populate the documents (see Case Study 1 on page 72) and even back to the manufacturer of the security paper in Switzerland to find out about the disposal of rejected sheets. As critical inputs to the

generation of certificates and reports, these were studied as sub-systems of a greater interconnected whole. The same principle bears upon the recruitment of new employees and also the acceptance of new customers. Due diligence processes are essential as these are both examples of significant inputs to the system that may escape consideration.

My use of process mapping is explained in more detail in the next chapter, along with illustrations of how I developed it over the duration of the project.

To analyse the data my project had produced and to capture its complexity and richness, I needed 'to comprehend and to theorize how people appropriate and enact their realities' (Brown, Colville and Pye, 2015: 265) with a particular focus on their perceptions of security risks. For this reason, as well as to align with the practical, problem-solving demands of my role as actor and active participant, I decided to employ a *case study* method as part of my analytical framework, alongside *sensemaking*.

Case study method

Case studies facilitate understanding of how people, groups and even the systems themselves make sense of unpredictable stimuli:

> Deep understanding in [case study research] includes: knowledge of 'sensemaking' processes created by individuals (see Weick, 1995); and systems thinking, policy mapping, and systems dynamics modelling (e.g. Hall, 1991) – what might be labelled appropriately as meta-sensemaking.
>
> Woodside and Wilson, 2003: 497

Of all the options, this seemed to afford me the best means of gaining 'in-depth understanding replete with meaning for the subject, focusing on process rather than outcome, on discovery rather than confirmation' (Burns, 2000: 460).

However, the case study method 'is typically criticized for being specific to the circumstances of individual practice and, therefore, limited in what it can offer theory' (Harland, 2014:1115). Gillham locates this problem within the notion of *generalisation* and notes that:

> … in human behaviour, generalisation from one group of people to others, or one institution to another, is often suspect – because there are too many elements that are specific to that group or institution.
>
> Gillham, 2010: 6

Yet Yin's observations suggest that this is to miss the point:

> Case studies, like experiments, are generalisable to theoretical propositions, not to statistical populations, and the investigator's goal is to expand theories and not to undertake statistical generalisation.
>
> Yin, 2009: 15

My goal was to find out if and how it might be possible to integrate security risk management into mainstream management and achieve a deeper, richer and more coherent understanding of security risks by working at the process level. This was, in essence, a theoretical proposition and its success would not be judged by statistical means. As my ontological position shifted from rationalism and empiricism to a more pragmatic perspective that emphasised workable solutions, I embraced the view that the case study method, 'unconstrained by the rigid limits of questionnaires and models … can lead to new and creative insights, building of new theory, and have high validity with practitioners – the ultimate user of research (Dul and Hak, 2008: xvii).

Sensemaking

I analysed the case studies using a form of *sensemaking*. This term refers to the ways 'by which people seek plausibly to understand ambiguous, equivocal or confusing issues or events' (Brown, Colville and Pye, 2015: 265).

> Explicit efforts at sensemaking tend to occur when the current state of the world is perceived to be different from the expected state of the world, or when there is no obvious way to engage the world. In such circumstances, there is a shift from the experience of immersion in projects to a sense that the flow of action has become unintelligible in some way.
>
> Weick, Sutcliffe and Obstfeld, 2006: 409

Sense and meaning are not just derived from observation, but also 'the interplay of action and interpretation' (Weick, Sutcliffe and Obstfeld, 2006: 409). Indeed, sensemaking is action – 'the active authoring of the situations in which reflexive actors are embedded and are attempting to comprehend' (Brown, Colville and Pye, 2015: 267). Sensemaking is therefore about organising information and this process is presented as a series of questions:

> Organizational sensemaking is first and foremost about the question: How does something come to be an event for organizational members? Second, sensemaking is about the question: What does an event mean? In the context of everyday life, when people confront something unintelligible and ask "what's the story here?" their question has the force of bringing an event into existence. When people then ask "now what should I do?" this added question has the force of bringing meaning into existence, meaning that they hope is stable enough for them to act into the future, continue to act, and to have the sense that they remain in touch with the continuing flow of experience.
>
> Weick, Sutcliffe and Obstfeld, 2006: 410

Sensemaking involves structuring or 'framing' our perceptions of stimuli and prevailing contexts together with developments or outcomes that we think these could produce. With experience:

> … this structuring becomes learning as agents cognitively detect regularities amid raw and often messy experience and compress these into less detailed conceptual structures that can then come to guide senses, inferences and behaviour.
>
> Holt & Cornelissen, 2014: 525

A key technique within the sensemaking process is *noticing and bracketing*. Writing about how a nurse identified that a patient's condition was deteriorating even though the cause was unknown to her, Weick, Sutcliffe and Obstfeld explain:

> Noticing and bracketing is an incipient state of sensemaking … [It] is guided by mental models she has acquired during her work, training and life experience.
>
> Weick, Sutcliffe and Obstfeld, 2006: 411

Hence, the observer may not have a name or terminology for the observed condition, but they are able to make sense of it because they notice the signs or symptoms and bracket them as indicative of something of significance.

Sensemaking can also be a team effort and has been applied to risk assessment and analysis in law enforcement, military and intelligence contexts with attempts to identify aspects of risk that are known, knowable and unknowable (Khanyile and Cluett, 2017: 1). It proved eminently suitable for my project and the data it generated, which was highly qualitative and contextual.

Summary

My project began with what I now define as the first phase of research that relied heavily on research methods derived from the positivist traditions. My selection of a self-completion questionnaire to gather enough information to inform my sample selection of venues for observational studies was founded on the premise of a single reality which I believed my chosen methods would reveal. At that stage, my use of process mapping was basic and primarily as a tool to aid my own thinking and my engagement with business experts and process owners. However, this tool and its application proved amenable to the shift in focus demanded by the changing priorities within my organisation. It progressively evolved into a full-blown systems analysis method which became an integral part of the security risk management approach that my project produced.

As my understanding of risk developed to embrace a more perception-based, cultural perspective, I needed to gain greater insight into the perceptions of process owners and those who manage them. My methodological approach therefore shifted to engage with a phenomenological and interpretivist perspective to extract the highest value contribution from those I observed and collaborated with during my field work.

I tested and refined my approach on a range of security risks and businesses that were either specified as a focus consequential to an incident that required investigation, or revealed during the course of my analyses.

Table 1 provides an indicative list of the main projects in which I developed my approach. It shows the primary business involved, the main risks the project addressed, the size of the collaborative team and the numbers of contributors to group work. The table is not entirely accurate because I often have several mini-projects emerge during my visits to which I would have also applied some aspects of my approach, depending on need. In addition, the numbers of focus group members often fluctuated as some people arrive late, leave early or get substituted by others.

Region	Business	Risks	Team size	Group size
Central America	Mining	Kidnap, fraud, organised crime	3-5	5-20
	Petrochemicals	Intimidation, fraud	3	6
Central Asia	Industrial	Fraud	3	20
	Agriculture	Bribery & corruption	4	15
East Africa	Petrochemicals	Bribery & corruption	2	15
Far East	Manufacturing	Bribery & corruption	2	10
	Pharmaceuticals	Espionage	2	8
North Africa	Textiles	Bribery & corruption	5	5
North America	Pharmaceuticals	Espionage	3	15-20
South America	Gas	Bribery & corruption, violence	3	20
	Transportation	Bribery & corruption	3	12
	Agriculture	Political violence	3	7
South Asia	Manufacturing	Bribery & corruption	2	25
	Pharmaceuticals	Espionage	2	8
Southern Africa	Mining	Fraud	4	12
	Petrochemicals	Bribery & corruption	3	18

Region	Business	Risks	Team size	Group size
Southern Europe	Mining	Theft	5	15
	Transportation	Bribery & corruption	4	6
West Africa	Agriculture	Theft, bribery & corruption	2-5	15
	Transportation	Bribery & corruption, armed robbery	2	

Table 1: List of candidate case studies

From these, I selected four case studies for inclusion in this project and these are presented in Chapter 7.

With the tools and methods presented in this chapter, I found a means of gathering and analysing data that was fit for purpose for the complex task I had set myself, and one that I could justify to both company and academic scrutiny.

CHAPTER 6: DATA COLLECTION AND ANALYSIS

This chapter provides an account of my experiences during implementation of the methodological approach presented in the previous chapter. Of particular importance are the descriptions of the problems I encountered and how these helped steer me towards more suitable methods.

Data collection

FAMDoc

Data collection started with the self-completion questionnaire which I sent, along with an explanatory note and glossary of key terminology, to those responsible for managing security paper in each of our Affiliates. Its purpose was to find out about existing document management practices and their views on issues that emerged from preliminary analysis of the documented reports and complaints. The questions concerned their production of the documents of interest, the types of entities or 'end users' that required them, whether a traditional paper-based format was legally required or simply an established custom, and their risk perceptions of various aspects and uses of the document as a legal instrument.

As the completed returns arrived, I encountered some unanticipated 'real world' problems when I started to collate the responses. First, some of the returns had not been completed by the intended respondent, the content I received indicated varying degrees of knowledge and understanding and it was difficult to establish the authority and credibility of the actual respondents, because it emerged that job and role titles were inconsistent between Affiliates. I also discovered that centrally held records were not kept up to date and there were inaccuracies in the information I had been given about business activities and the personnel responsible for them. There were also organisational protocol issues, as some Affiliates required everything sent from Corporate HQ (which I represented) to be diverted to the local Country Manager so that it could be delegated internally by that individual. Others had just delegated responsibility for managing security paper in an *ad hoc* way because they were simply busy.

Second, and despite my inclusion of a glossary, many respondents had either not understood or had chosen to ignore the 'operational definition' (Burns, 2000: 6) of key terminology. Some had answered my questions with complaints about safety or other issues, such as needing new vehicles to get to client sites or not having enough funds to purchase personal protective equipment (PPE), such as goggles and safety boots. Later, I realised that some of this was probably a consequence of a semantic misunderstanding, as the word 'security' translates from English to both *safety* and *security* in Spanish and other languages that use one word for both concepts (Talbot and Jakeman, 2009: 6) and some Francophone countries in Africa also interpreted 'integrity' as signifying *personal safety*. Translation issues notwithstanding, some respondents even took it upon themselves to edit the questionnaire by adding supplementary responses to questions I hadn't asked, because they wanted to use the opportunity to make points about other issues.

Normal research practice would tend towards rejecting such responses as null or – if the objections were significant enough – to re-design the instrument and to re-distribute. However, when I explained all this to my line manager, he told me that I had to work as best I could with what I had,

as there was a ‘big push’ for more revenue in progress and Affiliates were complaining about ‘questionnaire fatigue’ while being under pressure to focus on core business objectives.

Cracks started to form in my view of my new company as a tightly organised, highly structured and compliant entity, and my confidence diminished in the suitability of my choice of research methods. Nevertheless, I extracted and analysed what data I could from the questionnaire returns, then selected a stratified sample for follow-up visits, during which I intended to conduct focus groups, interviews and direct observations to delve deeper into the various systems in use. These would explore the examples that analysis of the survey data revealed, to allow me to gain ‘access to individual meaning in the context of ongoing daily life’ (Burns, 2000: 388).

However, having identified a suitable sample of destinations and after successfully conducting several research visits (one of which resulted in Case Study 1, presented on page 72), I then received notice that travel restrictions had been put in place until after publication of the annual financial results, so only ‘essential’ international travel was allowed. Put simply, I had to go where I was sent and to make the best of the research opportunities this presented me with, so I simply applied and tested my approach wherever I could. Fortunately, integrity investigations came under the definition of ‘essential’ so I could travel to conduct those, but none of the countries I was sent to thereafter were in my selected research sample.

Other challenges were soon forthcoming. Once ‘in country’ and with a complex investigation to conduct, I tried to set aside at least one whole day dedicated to FAMDoc project field research, but this was *always* disrupted by unpredictable operational demands. It’s important to understand that I was there – invariably on the other side of the world – as a member of an elite global corporate team that many Affiliates had never even heard of. If the relationship with the Country Manager was good, I would be asked to ‘have a look’ at an array of other problems that had not been reported previously – some of which directly affected the personal security of employees. It would have been ethically wrong and socially and politically unacceptable to decline such requests on the grounds of needing to conduct academic research. Further, some of the problems raised in this way developed into full-blown projects or investigations and included the South American gas testing case, featured in Figure 10 on page 68 and Figure 11 on page 69. It was in this way that the FAMDoc project started to evolve into BPSA.

I therefore had to multi-task and do my doctoral research field work ‘on the fly’, and it was rarely possible to maintain anything like ideal conditions for data gathering using my chosen methods. For example, I had drafted a semi-structured interview schedule for FAMDoc, designed to amplify the questions from the earlier self-completion questionnaire. However, during attempts to pilot, I could rarely complete it or even conduct interviews in what would normally be considered ‘reasonable’ conditions because of interruption or industrial noise. Similarly, I compiled lists of people to invite to focus groups based on their responsibilities and experience, only to find that some or even most couldn’t attend or had to leave early due to other unforeseen demands on their time.

I conducted field observations of relevant processes, such as the issue of security paper from central storage repositories, but my activities were often disrupted as I had to attend to multiple agendas regarding other issues at the same time. Sometimes I would be able to observe all the processes I needed to understand in sequential order, but often I had to conduct my observations

in bits and pieces and out of sequence, which disrupted the continuity and flow. These problems persisted into the next stage of the research, but I was better prepared as by then I had revised my methodological approach.

BPSA

While gathering my data for FAMDoc, my sample selection was disrupted, research instruments were tampered with, interview questions were ignored or re-phrased by respondents and everything got uncomfortably messy and I had had insufficient power to control the situation. In the BPSA stage, I adopted the bricoleur's approach and improvised.

The intended research methods for BPSA were background research, interviews, group work, observations and role-plays. The background research remained straightforward and involved fact-finding about the locations involved and the type of business that was at risk. This is a very important part of the research as it provides the context for all the other aspects that come later as each case progresses.

One of the main challenges in gathering the project data was overcoming my lack of technical knowledge about many of the myriad business activities my company undertakes. I developed a heuristic practice of seeking out 'the cooperation of many disciplines and professions' (Simon and Newell, 1958: 1) and finding one or more 'host' managers or employees in the locations I visited, to explain to me those activities I needed to analyse and to 'walk me through' the various systems of work. These were engineers, chemists, metallurgists, as well as legal officers, human resource managers and business development managers, as well as supervisors and front-line operational personnel. Over time, these people would become to varying degrees participants in my work as a process of mutual sharing and learning took place. I needed to engage them in what I was doing and find ways of explaining my own perspective in ways they could understand, and to encourage them to reciprocate and share their reality with me.

This was not simply a process of asking questions and listening to their answers. Workplaces are repositories of vast reservoirs of *tacit* knowledge. Tacit knowledge is expressed in the idea that 'we can know more than we can tell' (Polanyi, 1966: 4) and recognises that people and organisations have ways of doing things that are not codified in documents or even in orally communicated training. To uncover such knowledge, it is necessary to be present and active within the setting and to build trust.

When it came to interviews, I found that managers sometimes wanted me to conduct what I intended to be a formal interview over dinner, but would then arrive accompanied by other colleagues who they would sometimes invite to join in and contribute answers, so this became a focus group. I might later find out the manager's personal view on a topic through a revelation during the drive home, or others might open up to me during a taxi ride to the airport or over a drink in the business lounge. All such information had to be integrated into the data set.

Similarly, although sometimes had the opportunity to run conventional focus groups, I also built discussions about security risks into training and awareness sessions and conversations with clusters of managers whenever possible. I also made as much use as possible of the multi-disciplinary team work, and these discussions were crucial to building and testing process maps.

There was a high degree of informality about many of the interactions. Nevertheless, the information I took away was useful and provided me with valuable insights, as well as material to discuss with others at the next opportunity or when similar circumstances to those discussed arose.

When it came to process mapping, I found that those businesses that are intensely process-oriented incorporate such techniques to varying degrees of granularity at the design phase, so process maps or similarly detailed overviews were available for study and analysis. For those that did not do this, I created the maps in consultation with members of the team formed to address each project.

The group work involved in the process-mapping exercise was absolutely fundamental to the project because it encouraged – even forced – participants to think about the business on a different level. I opened these consultations by explaining my project and its aims, and then simply asked the question 'what happens first?'. Using a whiteboard or similar (I once used a stick to draw in the dust in one West African country), I would sketch a process and suggest a label for it, then work forwards – and sometimes backwards – from that point while eliciting further information from the group. Adapted from medicine, this is a sensemaking technique known as 'functional deployment':

> In organizing in general, functional deployment means imposing labels on interdependent events in ways that suggest plausible acts of managing, coordinating and distributing.
>
> Weick, Sutcliffe and Obstfeld, 2006:411

I recorded the data from group work and interviews in process map sketches. Figure 7 shows the results of a workshop held in a large port in East Africa and concerned the production of certificates and reports from the inspection and testing of petrochemicals.

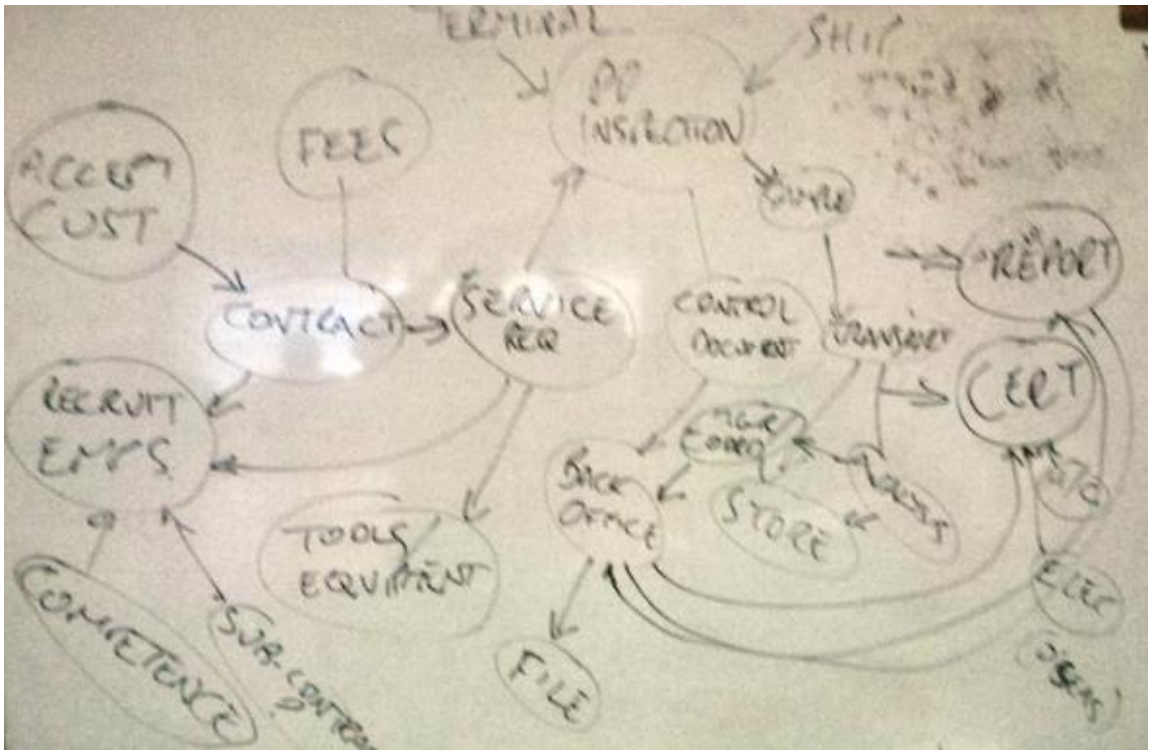


Figure 7: Draft process map (petrochemicals in East Africa)

While mapping the processes, I ask participants to explain which inputs each process needs to operate and which outputs they produce. As intimated earlier, inputs could be hard or soft, but the outputs they generate carry the combined inputs of the process that produced them into the next process. Here, quality management theory applies, because this can have both positive and negative cumulative effects, as either value is added or errors and bad intentions are compounded as the system proceeds. Inputs and outputs can also include risks and protective controls and employee interactions also revealed their risk perceptions.

I would photograph my whiteboard sketches then refine and simplify them for presentation – along with the photograph of the original – to senior managers. This was intended to provide an overview and suggest a visualisation of a generic model of essential processes found in every certificate and report production system, as shown in Figure 8.

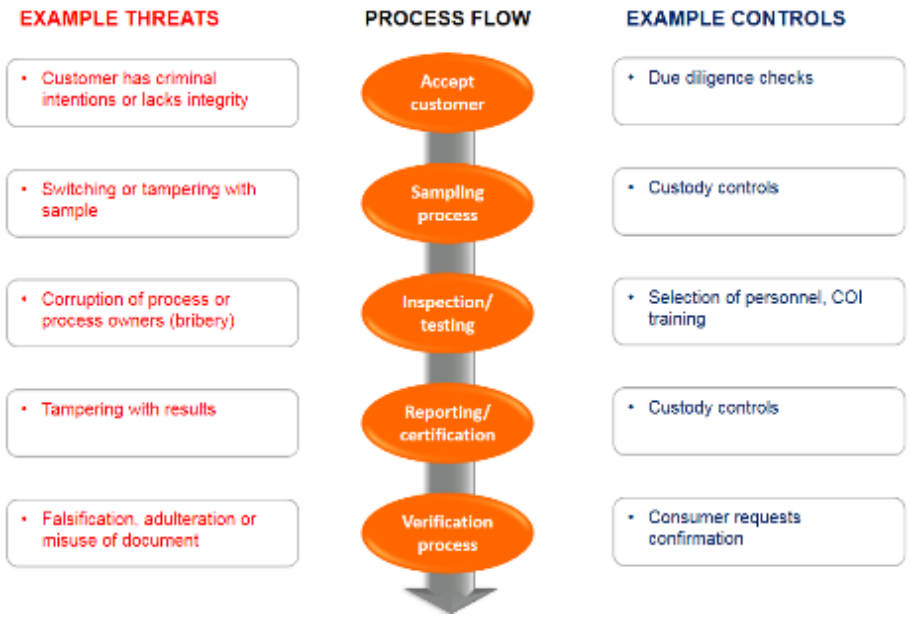


Figure 8: Process map for management

Figure 9 shows an attempt to make sense of and express the security risk aspects of two parallel processes, using human language sentences that incorporate the criminological concepts of *targets, threats, motives* and so on.

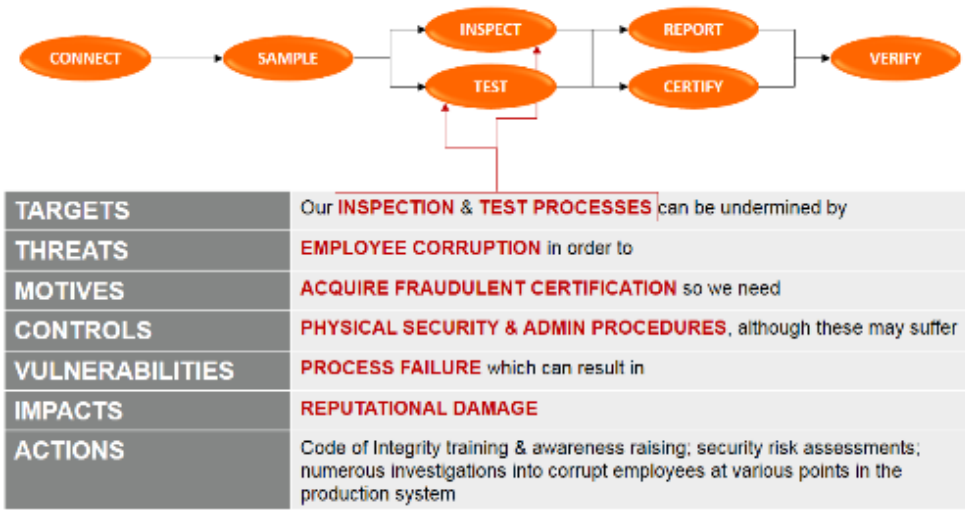


Figure 9: Systems map with risk assessment at process level

I produced similar graphics and structured sentences for each process as a vehicle for discussion. This would then generate questions related to the classical definitions of risk as a relationship between probability and impact, sometimes with an attempt to give these numerical values. However, although the discussions were good, the numbers were meaningless outside the context of that meeting or session. One person's 10% is another person's 30%, so it's just as valid to use 'high', 'medium' and 'low'.

The first case I conducted after FAMDoc became BPSA appears as Case Study 2 (page 80) so that is discussed later. However, the example shown in Figure 10 is also from the early weeks of the BPSA stage and pertains to domestic gas supply testing in the capital of a South American country. As mentioned earlier, this case was not the reason I was in the country concerned, and was suggested by the Country Manager almost as an afterthought over lunch. Such occurrences are not atypical in my role and this example further illustrates the challenges to orderly project planning that I faced.

However, a focus group of gas inspectors and their supervisors identified five main process clusters shown as orange ellipses. The term 'clusters' refers to a group of closely related processes that could be deconstructed as individual separate processes, but the value in doing so may be marginal. There was a business process map already in existence, but everything shown in Figure 10 appeared as a single process called 'OPERATIONS', so this chart represents a much more granular analysis than previously existed. The blue text represents equipment or locations that pertain to each process, while the red text shows perceived risks, based on group members' experiences. The chart was originally presented in the local language.

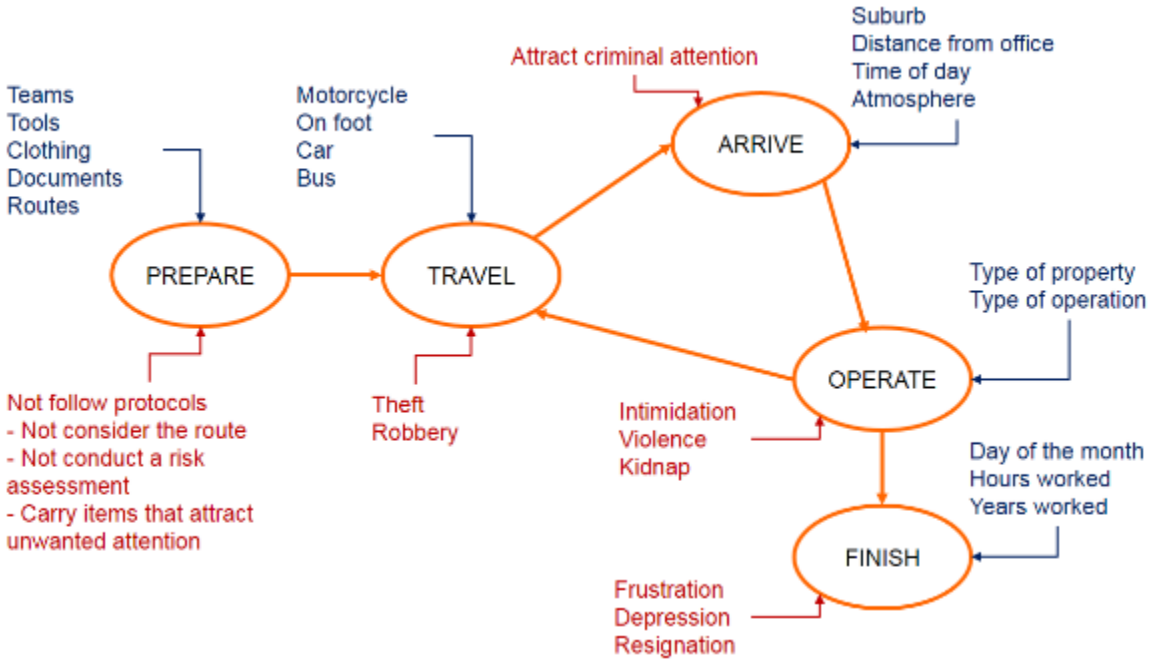


Figure 10: Process map - domestic gas supply testing (South America)

Presentation to managers using these techniques was also a continuation of the data gathering exercise, as I needed to capture their comments and insights into their experience because they understood how a deceptively small issue could have a significant impact on the business. They were also able to discern whether employees were working as they should or if they were

bypassing checks and controls. For my part, I was able to use these sessions to introduce them to core concepts in security, such as situational crime prevention and the concept of displacement. This allowed them to help me identify any displacement risks elsewhere in the system.

I later started to produce process maps using Microsoft Visio software, which is an 'industry standard' tool that also provides a visual means of associating processes with their owners. Examples appear within the Case Studies 3 (page 88) and 4 (page 100).

During observations, and when appropriate (and legal (some ports and similar facilities forbid it), I made extensive use of photography to capture data. Photographs are a wonderful tool for sensemaking and are invariably more practical than notetaking, especially in high risk environments or those where it was necessary to wear protective equipment.

Figure 11 shows a gas inspector working for the business discussed around Figure 10 as he enters a basement apartment. The adjacent photo shows him completing his inspection report inside the residence. He would normally do this alone, leaving him exposed to a range of security risks. As referenced in the process map on the previous page, some employees have been held hostage by residents after disconnecting their gas supplies for safety reasons (one was subjected to live-streamed humiliation and abuse on Facebook), while others have been accused of sexual assault.

Figure 11: Participant observation (South America)

The insights gained from these methods allowed me – in consultation with the relevant process and system owners – to generate ideas for security and integrity enhancement, as well as to reflect on alternative ways of attacking the system, possibly exploiting other processes that were unintentionally weakened by correcting newly identified vulnerabilities. This was part of the evolving analytical framework, derived from the core disciplines presented in the literature review.

Data analysis

Each operation or 'job' produced a report for my internal customers to explain my activities and methods, present my findings and my recommendations for improvement. These generated two types of case study: complex and simple. Examples of the complex variety are included in the Case Studies chapter of this report and are shared with senior managers to inform decision-making at that level. I used the simple type as the basis of short discussion pieces for managers and

operational employees to illustrate common 'scripts', often with an integrity theme related to bribery, corruption or intimidation risks. This forms part of the dissemination strategy for the project which includes a range of approaches to raising colleagues' awareness of security risk management.

As mentioned in my methodology, I used a simple form of *sensemaking* to analyse the highly qualitative and contextual data that the case studies generated. I adapted this process to fit the theoretical framework I presented in my literature review.

First, I ask the question in various forms, how does something come to be a *security risk* event that could affect our business? What opportunities for acquisitive crime are present? What damage could a disgruntled employee cause? What would happen if a manager abused their authority? Are any of these factors perceived by those involved? Do they occur in their narratives or is there any indication that they try to conceal them? What indicators are present that we can interpret as a cue for action? Some of them may be hidden in the detail. Weick observes:

> Students of sensemaking understand that the order in organizational life comes just as much from the subtle, the small, the relational, the oral, the particular, and the momentary as it does from the conspicuous, the large, the substantive, the written, the general, and the sustained.
>
> Weick, Sutcliffe and Obstfeld, 2006: 410

We can identify the assets and processes that could be targeted for various reasons, and we have some criminological understanding of possible offender motivations.

Second, what does or would such an event mean or, put another way, what would be the impact? We can assess this in terms of direct and indirect financial losses and reputational damage, as well as functional impediment. This may occur if a rare piece of equipment or similar resource is stolen or destroyed, or if employees are afraid or demotivated because of a perceived risk to their well-being. To answer this question, we need to hear the authentic voices of those affected. This demands a detailed and granular approach, so I try to establish what each process uses and generates, then explore how this is or may be perceived by those who want to protect it and those who might attack it. However, it is also vital to locate each process within the greater whole, so the creation and structure of the process map forms a crucial part of the analysis.

Third, what can we do about this and what impact might our actions have. To answer this, I need to know what we already do, which involves identifying and decoding the control system. I look for *tactical* controls, such as security technology, guards and passwords, and *political* controls, such as policies, procedures and rules that govern how such measures are applied. I also look for *cultural* controls, drawing from management theory to identify management style and power dynamics, and the constitution of teams and groups. We also have a temporal framework that allows us to manage the event before it manifests itself as an incident, in the hope that we can prevent it or reduce its impact. If this fails, we can resort to other points of intervention. Are they 'risk-aware' and do they 'notice' and 'bracket' the symptoms that new risks may be present?

These sensemaking questions are asked in a rolling cycle as each process within the system of work is studied and assessed. The evolving process map assimilates the knowledge and

perspectives shared by participants until we can say with some degree of confidence that 'we get the picture'.

Summary

I began my project with the belief that I would find a much higher degree of consistency within my global organisation in terms of policy and terminology. I expected clear, centrally-formulated standards, a culture of compliance with documented norms, and stringent enforcement measures. Had this been the case, my data collection and analysis would probably have been relatively painless and certainly more amenable to the methodological approach I began with. Instead, I found a 'light touch' culture that delegates policy formulation – especially concerning security – from the global, corporate level to the Affiliate level. This has positive aspects, in that it capitalises on the knowledge, expertise and sensitivities of local management and allows – indeed requires – Affiliates to orient themselves to local conditions. However, it also creates a lattice of complexity and inconsistency that is difficult to penetrate using the social science tools I had chosen.

The initial data gathering process was fraught with problems, but this was as much to do with my own unrealistic expectations, probably derived from past research experiences which had been relatively 'tidy'. However, the research process became easier and more familiar as I learnt to accept that the 'rough edges' were part of the phenomena I was trying to understand – and part of the experience that others would experience when using my approach for themselves.

The next chapter presents four case studies to illustrate how all of this was put into practice in the field.

CHAPTER 7: CASE STUDIES

This selection of four case studies is presented in chronological order to show how the approach developed over time. All four are genuine examples of security risk management problems with the potential cause serious consequences for my company, its employees and also the wider community.

The first study, conducted in 2013, was the first application of my approach to reach beyond the production of certificates that was presented in the Methodology chapter. It still formed part of the FAMDoc project, but it involved expanding the scope of the enquiry to study the production of data that certificates and reports contain. It also identified weaknesses in the processes by which my company accepts customers as genuine commercial entities.

The second study focuses on bribery and corruption in a 'B2C' (business to consumer) service, which in my company are in a minority (although the domestic gas testing mentioned earlier is another example) because most of our work is in the 'B2B' (business to business) space. Here, the analysis helped identify a means of measuring the size and scale of the problem and using this means to establish new 'integrity performance' measurement for employees whose roles exposed them to risk. This study was also the first to be conducted as a joint operation, in the case with a technical governance specialist concerned with best practice in the business processes.

The third case study is one of the most ambitious I conducted during my doctoral field work and was also the first time I applied my approach in a commercial, customer-facing context. The project was highly complex, involving collaboration with a team of mining experts in plant and laboratory operations. BPSA was adopted as the primary approach for the entire study, which concerned quality and efficiency aspects in addition to security risk management.

The fourth case study is from 2016 and is included to show how BPSA started to integrate generic management tools – in this case, the McKinsey 7-S Framework – as it burrowed deeper into organisational relationships and business processes.

BPSA is now a standard approach within my organisation and these four cases represent about 10 per cent of the projects where I have used it. Other applications were in petrochemicals, food, transport and shipping, agriculture, social auditing and pharmaceuticals.

CASE STUDY 1: Minerals trade services in Latin America

The case study presents a security risk assessment of a minerals trade services laboratory located in a port-based branch of a Latin American Affiliate. The main business of the branch was the preparation of minerals samples prior to analysis and certification by a centralised geochemistry laboratory in another location. The analysis would determine the value per tonne of the shipment, which often ran into millions of dollars, so there was plenty of incentive for criminal manipulation of the system.

A security risk assessment was officially requested by the Country Manager after a supervisor was dismissed for drinking alcohol in the workplace, but I had also selected the country as part of the preferred sample for the FAMDoc project. This was therefore a welcome coincidence, despite the circumstances. The stated purpose of the assessment was to focus on any security risks related to

the production of certificates and reports. However, various rumours were circulating within the Affiliate about serious organised criminal gangs in the area and concern was expressed about the professional integrity and personal security of employees. The underlying context of the assessment was therefore multi-layered.

Setting and context

As mentioned earlier, environmental criminology and situational crime theories explore links between criminal behaviour and the surrounding environment, so I always begin an assessment with a short study of the location – especially if I'm unfamiliar with it. In this case, the Latin American country where the branch is located suffers from high crime and chronic poverty, especially in rural and inner city urban areas. At that time, unemployment was high and the country was enduring major problems with law enforcement in many regions. Corruption was known to be rife at all levels of society, yet the economy was growing and investment was flowing in, due in part to the country's mineral wealth and an abundance of other natural resources, as well as the growing ambitions and capabilities of its people.

Business type may also have some influence on the propensity for criminal behaviour against it. Minerals trade services is a tough business that often operates in high risk areas throughout the world. The most significant customers are the large multinational corporations that trade in minerals, but there are also many small mining companies in the sector. In this location, some of these were alleged by industry insiders to evade regulatory controls and engage in 'sharp practices' to benefit from investment or other support from organised criminal groups (OCGs). Such groups sometimes purchase such companies to present an apparently respectable face to the outside world and to facilitate diversification from narcotics, weapons and people-trafficking to other businesses, including the mining and minerals sectors.

In terms of the location itself, the branch at that time was a substandard facility on a small industrial estate. It had no access control to its outer perimeter and, as shown in the photograph, carried out various operations in the open air. However, its position next to a large international freight port handling shipments of general cargo, minerals, agricultural products and containerised products was commercially attractive. At that time, minerals accounted for around 20% of the port's throughput, having increased by over 10% in the previous three years to around 5.2 million tonnes per annum. Media reports on high-profile seizures of incoming and outgoing contraband indicated that this growth was attracting unwanted attention from OCGs.

On arrival at the branch, I organised a focus group to help me map the system, identify the threats and discuss the risks. The group comprised the branch manager and his deputy, with occasional contributions from the national Business Manager who was accompanying me on the trip, but had other commitments and couldn't remain present all the time. I asked for some operational employees to be involved, but was told that none were available because of the volume of work. As

my project proceeded, I found this kind of response to my visits to be quite typical – unless I was conducting an investigation, in which case I could be more insistent. On fact-finding missions, such as security risk assessments, I had to be pragmatic and settle for the heuristic approach.

After the meeting, I conducted various observations at the location, and visited several *patios* or stockyards in the port where our inspectors collected samples and provided other services.

Key findings

The discussion produced a process map (Figure 12) that indicated that various processes provided opportunities to tamper with, switch or steal samples.

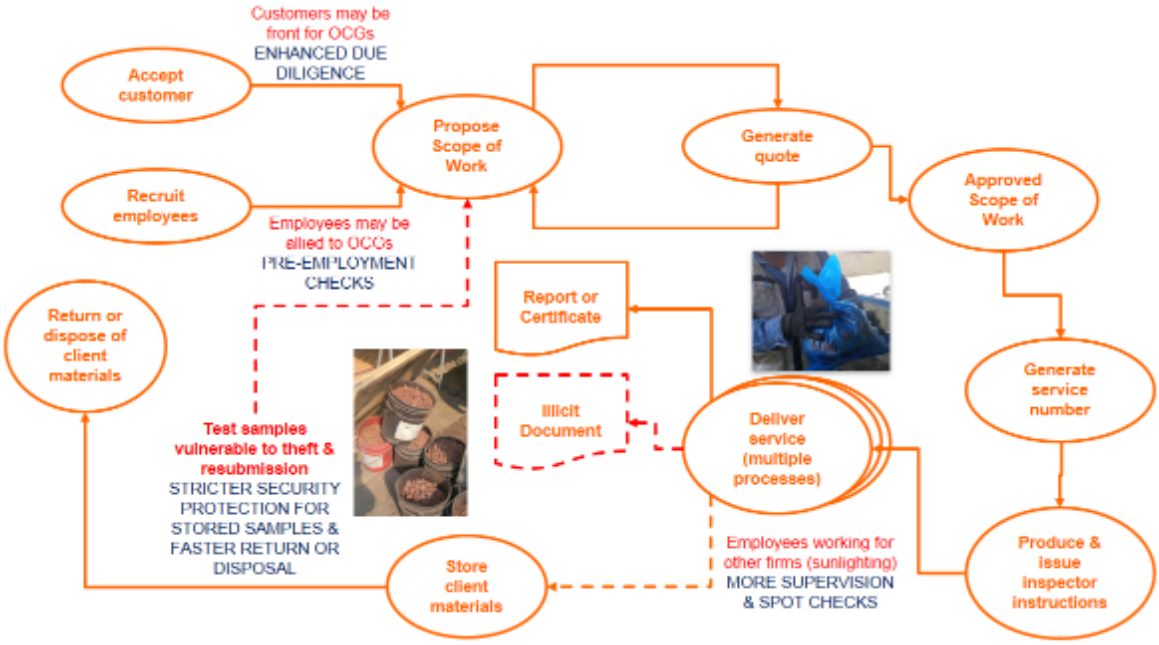


Figure 12: Minerals Trade Services Process Map

The assessment identified many types of threat to the business, but I will limit the discussion here to two specific issues that were particularly helpful and exciting revelations in terms of my project. The first concerns the theft and manipulation of customer samples. These are small quantities of mineral concentrate that are gathered from the trucks that bring the material from the mines that produce it to one of the many stockyards in the port area.

Of particular concern was theft from the 'store client materials' process at the bottom of the diagram. The focus group concluded that this was probably the most vulnerable and highest risk process in the system. This is because both unprepared and prepared samples are stored with a unique identifier that ties them to the results that are returned following analysis. As shown in the photo, unprepared samples are left unsecured, so offenders can easily remove part or all of the content. However, the motivation for stealing a bucket of dirt wasn't immediately obvious and I had to press the group to think hard about why someone would want to do this and what benefits they could derive. What emerged was a complex risk picture that extended beyond our company, but within which this branch appeared to play a small but pivotal role. To understand this, it is necessary to have an overview of how samples are gathered and processed.

Minerals samples may be gathered either by our employees or by another party, such as a trader or the stockyard owner. In the latter case, we cannot vouch for the sample gathering process and this will be stated on any certification we issue following analysis. However, if our employees gathered the sample, then we remain accountable for all the associated processes.

After gathering, the sample is labelled and carried by road to the port branch for preparation, prior to being dispatched for analysis elsewhere. Any remaining sample material is labelled and stored, ostensibly for re-testing in the event of a dispute. Analytical testing reveals the mineral content of each sample, which determines its quality and has a direct effect on the asking price for the whole batch. Once the quality of a sample is known, further samples from the same batch can be submitted, safe in the knowledge that they will yield the same results. Anyone who has access to the original unprepared sample could do this under a different identity than the rightful owner and claim that the sample was from a batch of inferior quality. So long as this customer's business is accepted by my company, the sample would be prepared and tested and would produce the expected results and a genuine certificate of quality.

Although the documentation would make it clear that the sample had been gathered by the customer (not my company, which would avoid the risk of a successful claim for compensation), an adept offender could obfuscate this detail and try to convince a third party – possibly a buyer, but more probably one or more financiers – that they had a genuinely valuable product that was worthy of purchase or investment. Hence, the primary threat is one that targets another entity, but uses my company as an unwitting accomplice to gain trust.

This was exciting because it revealed a new form of attack on our documentation and an alternative approach to falsifying or altering an existing certificate of quality, thereby reducing some of the risks of detection. It resonated with some previous work I had participated in (Hart and Evans, 2012) on the assumption of new identities by terrorists and other criminals and how they abandoned attempts to use counterfeit passports because the security measures in genuine documents were too difficult to defeat. As another example of displacement, they chose to attack a different part of the passport or ID card production system to acquire a 'fraudulently obtained genuine' (FOG) document using fakes of other, less secure 'breeder' documents, such as bank statements and utility bills.

We would not have identified this criminal opportunity without the systems approach I was developing.

The second issue I will highlight concerns my company's exposure to 'illicit customers', i.e. criminals who exploit the 'accept customer' process to facilitate some form of criminality. Using as a metaphor the defence-in-depth approach favoured by military security specialists, this process and the 'recruit employee' process that runs parallel to it, provide the first line of defence against infiltration of our system. Failing to conduct appropriate due diligence or pre-employment checks in order to know who one is doing business with exposes the company to various forms of insider threat.

In this case, the business acquired customers via various routes, including referral by HQ, in response to sales initiatives by business development personnel, by direct application for

assistance via an online enquiry form or simply by someone visiting the branch in person to bring a sample for testing.

While global HQ owned the risks associated with accepting large international clients, those associated with local companies were divided between the Affiliate HQ and the branch. To be registered as an Affiliate-approved customer, new clients must provide some basic fiscal information, including a registered address, telephone number and other basic details, as well as a tax identification code to show their legal status. However, subject to his own judgement, the local manager had latitude to undertake work for local companies or individuals who had *not* undergone this process – so long as the customer paid cash in advance.

This presents a significant opportunity for someone with illicit intentions, but not enough of one to meet the needs of an organisation planning a more strategic fraud, for example by building at least a minimally good reputation first. While the local Affiliate's Finance Department owns the risks associated with accepting a potential customer as a legal entity in that country, it does not have instructions or the capability to investigate the integrity of all the relevant data it will receive. Other checks related to their ability to pay may take place later, but all first transactions require payment in advance. Put simply, these checks provide a minimum level of legal and financial protection for the company – and they help ensure that we get paid – but they don't tell us much about who we are working for and offer little protection against a planned intentional attack of the sort under discussion here.

Again, the systems approach succeeded in identifying vulnerabilities that the business was unaware of. In the following months, similar vulnerabilities were found in other businesses in other locations and were able to learn from this experience. One example was an Affiliate in a West African country where we accepted cash-in-advance samples from artisanal miners. As the government had decreed that all mineral wealth was the property of the state, artisanal mining effectively became criminalised, so we could have been accused of aiding offenders by accepting this work. As a direct result of this kind of systems analysis, the business was able to reconfigure and only accept work from suitably approved clients.

Other issues that emerged from this case study concerned the workplace culture and informal power structures that had been allowed to emerge. The 'accept employee' process is initiated by the business and authorised by the head of HR in the local Affiliate. All prospective inspectors and others trusted with similar responsibilities must agree to checks on their references, credit history and to an interview process to determine their good character, as well as medical checks for substance abuse and submission of documentation regarding any criminal history. However, in this country and others like it, the reliability of official data sources it highly variable, and references for individuals from small towns or rural areas are known to be likely to be written by members of the applicant's extended family. In addition, many lower level employees are recruited without having received prior training, and some of them told me that their training at the branch is largely 'on the job' and delivered by supervisors or peers. This – and a noticeable gulf between office-based managers and field-based workers – exposes new employees to being drawn into a wolf-pack as in Mars' (1984) study (see Figure 3 on page 40) resulting in continuation of ongoing unethical and criminal practices. Indeed, this scenario was subsequently confirmed by a different investigation.

Recommendations

The focus group eventually agreed that the overall risk of a major fraud occurring was of low probability, but very high impact. However, there were other less tangible and more probable consequences that emerged from this scenario and any similar situation where control systems are weak. Ports are communities that often use word-of-mouth communications to share experiences and spread rumours, so a company's reputation can easily be tarnished without a major scandal. In addition, situational crime theories remind us that weak controls also create opportunities for other forms of offending, such as petty theft of tools and consumables that can easily be sold on in a high crime environment with little chance of detection. It is unlikely that these opportunities had escaped the attention of operational employees.

These conclusions would not have been reached without the focus group and process mapping exercise, and this reveals some interesting insights about the risk perceptions of participants. Those responsible for operating the service delivery system had no thinking tools to identify and assess risk, so their risk perception was either low or 'unstructured'. I use this word because, it was clear that at least the branch manager – whose was born and raised in another region – was anxious, even afraid of the port and surrounding province, but he hadn't been able to consciously connect this to his working environment. His deputy was local and didn't seem afraid, but neither was he conscious of the vulnerabilities within the system. Subsequent conversations I had with the global leadership indicated that risk management played no part in the business design, as this was considered an 'operational issue' that had to be addressed in each local setting. However, there was no acknowledgement of this in the business documentation, which hardly addressed security risks at all.

However, working together, the focus group was able to formulate a three-part plan to manage security risks in the specific context of the environment, the system and the identified risks.

1 - Protect the system

Applying Routine Activities Theory, motivated offenders were known to be present but the value of the target was not properly understood by the system that was supposed to be its 'capable guardian' (Felson and Clarke, 1998: 4). The business needed a more formalised and documented approach to its operational systems and their monitoring and control throughout.

All new customers should be subject to a due diligence process. This may be driven by risk perception if managers have concerns or by random sampling if the volume of throughput is very high. Whichever method is used, greater clarity is needed about ownership of the risks associated with this key process

Regarding employee recruitment, the effectiveness of pre-employment checks should be assessed by comparing their results with employees' subsequent performance. The unfortunate event of a disciplinary action or dismissal provides a good opportunity to compare the employee's performance with that predicted by the pre-employment assessment process. All temporary employees and the companies that provide them must sign their understanding and acceptance of the Integrity code

Control systems should both deter wrongdoing and detect when it occurs. Enhancing security by reducing opportunities for both undetected error and intentional wrongdoing should be part of the quest for business performance and this needs to be applied throughout the value chain.

Processes should be protected by an appropriate level of physical and procedural security in recognition of the attendant risks. The unique ID that samples are given via the number seal should be put to better use, enabling managers to monitor (in real time and retrospectively) how material progresses through the system. In the interests of efficiency, accuracy and transparency, sample processes should be documented using an electronic system, rather than handwritten notes. This may require some staff training, such as in the prep lab which currently makes no use of computers. As the business grows, there may be a case for investing in inventory management technology, such as bar code capabilities

2 - Control the work

The relevant manager must ensure the scope of work covers all the processes required to complete the job. Details on how sampling must be conducted are already quite comprehensive but more detail on how samples will be secured during transportation may enhance customer confidence. Details on processing methods are clear, but storage and disposal, including maximum terms and any penalties for exceeding storage periods should also be clarified in this document

The process of converting the scope of work to clear operational instructions for Inspectors and other process owners needs attention. Conversion often requires translation and this should be done competently and this process also requires understanding of the sample, transporting, storage and disposal and other processes. Operatives should have no ambiguity about what is required of them and should require supervisor instructions before modifying these in the field

Sample size should be reduced in the field to make them easier to manage and transfer some of the initial prep lab tasks to the Inspectors. After gathering the sample, inspectors could undertake some initial filtering operations in the field. This would reduce sample size, rendering them less attractive to thieves, and would enable faster throughput at the prep lab. Samples should be transported in locked boxes with keys subject to the same inventory controls as office-based secure storage facilities

Sample reception and documentation needs tidying up. Custody of samples should be documented with clearly noted transfer of ownership as material moves through the system. Organisation of the sample warehouse needs revising so that any sample can be retrieved easily and samples due for disposal can be managed out of the system in an efficient manner. Access to the sample warehouse should be restricted with clear accountabilities given to the area supervisors

3 - Manage the people

The operating culture contrasted sharply with that of other parts of the minerals business, such as the analytical laboratory. Such facilities are usually staffed by highly qualified science graduates with a ‘white coat culture’ that reveres process, procedure, professional codes and a commitment to excellence. In contrast, the prep lab in the port branch had a ‘blue overalls’ culture with very few documented procedures, no formal qualifications and poor systemic controls.

Inspector and other employee training should be formalised and at least partly delivered in a classroom setting to ensure coverage of all necessary competences and incorporating any improvements identified by ongoing review. Ongoing review to identify opportunities for continuous improvement is essential from a security perspective, as threats are likely to evolve as the Port grows and becomes more attractive to criminal gangs. Inspectors and other personnel at the same level do not receive high pay, so providing them with some form of professional development, ideally with a pathway to supervisor status has many benefits for the company – not least in helping maintain loyalty and ethical compliance

Integrity code training should focus on the specific risks that Inspectors are likely to encounter in their role, providing an opportunity to prepare them on how to deal with unethical approaches, how to report incidents and the consequences of non-compliance. Severe consequences are less important than the certainty of detection, so the control system should provide convincing evidence of its effectiveness in this regard. This said, 'management by fear' has many negative consequences and will motivate competent employees to leave.

In addition, the branch manager and his immediate team need to better engage with the operational teams on a daily basis. There was a leadership vacuum that either appointed supervisors or 'natural leaders' within this group can fill. This was certainly the case with the recent thefts.

All processes should be subject to ongoing or spot-check supervision, as appropriate. All temporary workers must be subject to ongoing supervision by at least one full-time company employee. Adequate numbers of supervisory employees must be deployable to maintain a credible preparedness for spot-checks. Management level employees must also engage in spot-checks, of both supervisors and front-line employees. Spot-checks should be as much about positive reinforcement and support as detecting non-compliant actions.

To conclude, this case study extended the systems-based approach beyond the narrow scope of certificate production to the processes that precede it. The mapping focussed on the 'hard processes' that are relatively easy to identify, but the surrounding analysis also picked up on organisational dynamics and leadership issues. However, I had not yet started to use the McKinsey 7-S framework to explore these in more detail.

Sensemaking summary

In this wrap-up section, I summarise the answers to the three sensemaking questions from the analytical framework.

How does something come to be a security risk event in this business?

This case found that commodities perceived to have little or no value (in this case, minerals samples) are easily neglected unless documented procedures and associated requirements are put in place for their safekeeping. Criminals are quick to identify opportunities that remain hidden or obscured to people with a different mindset, especially if the rewards outweigh the risks, as was found here.

What impact would it have?

In this case, the theft of the waste materials that had already been tested was motivated by the desire to obtain a genuine certificate of quality to perpetrate a fraud or deception against another party.

What can we do about it?

Our existing controls were all about making sure we get paid, but do not provide the protection they could and should from the risk my analysis identified. Due diligence checks on new customers need to be much more thorough, and customers should be re-checked periodically to identify any new owners, shareholders or prominent employees. In addition, poor quality pre-employment checks left the door open to criminal infiltration of the branch, facilitating a significant 'insider threat' that was confirmed in a subsequent investigation.

This case study provides a good example of the consequences of isolating the security risk management function from operational realities that I wrote about in the introduction to this report. Local managers have technical knowledge, and they do have access to security expertise if they need it, but they don't know that they need it and nobody tells them otherwise.

CASE STUDY 2: Statutory vehicle testing in Eastern Europe

My company has provided statutory automotive technical (roadworthiness) testing services since 2009 on behalf of the Ministry of Transport in the Eastern European country where the case was situated. The Affiliate runs a concession of fifteen testing centres located in various towns and cities, the largest and most modern of which is just outside the capital city (referred to here as 'TC1'). The test centres vary in size, design and capacity, but all must be able to receive all classes of vehicles to the standard stipulated in the government contract.

The Country Manager asked for assistance after a consumer affairs programme made allegations on national television that vehicle inspectors routinely accepted and demanded bribes. They had shot some covert footage, which was later used as evidence to justify several dismissals.

However, as this was unlikely to be an isolated incident, I was asked to work with a technical governance specialist from the global business to address both integrity and operational efficiency and to recommend changes. This was also the first time I had received a formal request for a joint enquiry of this kind, and this pleased me because it represented a positive response to my exhortations to promote proactive security risk management and integrate it with other forms of service management and control. In this project, the two perspectives of technical governance and security risk management were to be harmonised in a coherent plan of action. This case study was also the first that I conducted in stage two of my project using the BPSA brand.

Four test centres were selected for review: TC1 and TC2 (both in the capital) and the provincial centres TC3 (North) and TC4 (South). These were chosen to present a range of operating environments, capacities and staffing levels and the largest volume of business. Staffing levels were known to be particularly significant to the management of internal threats because they affect each centre's ability to maintain appropriate separation of duties and responsibilities.

Setting and context

This country has a complex social, political and cultural history which contributes to a security risk environment where many forms of criminality continue to flourish. Violent incidents, armed robberies and revenge shootings are common, and there is a culture of organised crime founded on family and territorial affiliations. This sometimes manifests itself in workplaces in the form of nepotism and organised scams, as well as a reluctance to use reporting systems responsibly.

Like most others in the region, this country suffered repressive totalitarian control for many decades, although the planned economic model embraced by its rulers masked a thriving informal economy of illicit markets and routine official corruption. Despite a steady rate of improvement since democratisation, various serving and former security officials who I met with explained to me that bribing public officials for all forms of service continues to be deeply engrained in daily life.

The situational characteristics of the test centres facilitate bribery and corruption as the physical layouts allow co-mingling of customers and various businesses with centre staff. In addition, test centres are usually located in out of town sites and are surrounded by other small businesses, most notably small insurance kiosks – sometimes numbering over a dozen – and a few cafes. Insurance sales people routinely tout for business among waiting customers, who typically spend over one hour at the site when they will pay their vehicle tax and possibly by insurance while waiting their turn to have their vehicle tested. The Affiliate MD was convinced that many insurance vendors offered illicit incentives including a ‘guarantee’ that vehicles would pass the roadworthiness test in return for insurance custom. Anecdotal reports of test centre employees visiting coffee shops to negotiate commissions and receive cash payments from such individuals were common. Such incidents were also occasionally captured on CCTV.

Key findings

It wasn’t possible to assemble any group work on this job because of language difficulties and the availability of personnel, so I conducted a series of interactive interviews and physical observations of work taking place to produce a process map for each location. Figure 13 shows the process map for TC1, presented above an architectural plan of the location. This takes advantage of the fact that everything happens on a single site and enables the processes to be visualised approximately in line with the space where they occur. Other test centres operated in a similar way, but had fewer lanes and less capacity. Further, TC1 was responsible for over 60% of the business nationwide, so I will limit my discussion here to this one location.

The orange bubbles are processes, the text in red describes risks, while the text in blue represents recommended security and integrity controls.

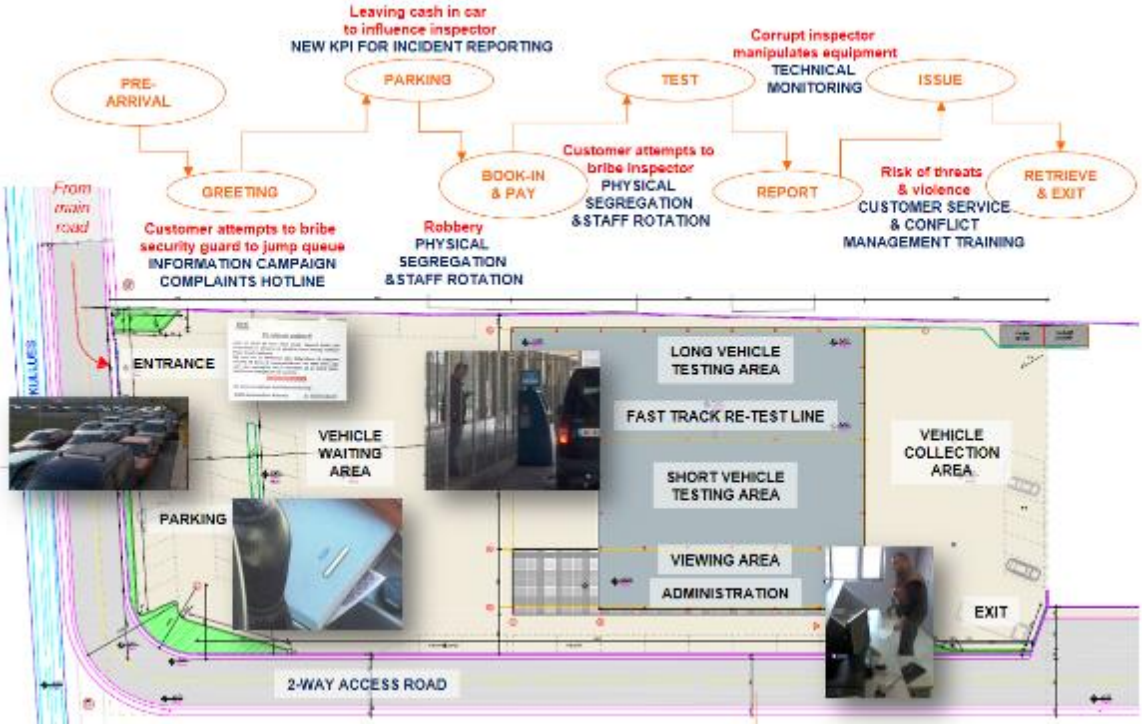


Figure 13: Statutory Automotive Testing Process & Location Map

As with the previous study, the assessment found plenty of opportunities for security enhancements, but I will focus here on the most eye-catching findings. The first concerns my development of a system of metrics to measure the integrity performance of each employee whose role put them at risk of bribery. All the human sources I had contact with complained that corruption was 'rife', 'endemic' and even a 'natural' form of behaviour for the local nationals to engage in. However, nobody could indicate the size or shape of the problem – they simply maintained that 'it's all corrupt – everyone's corrupt'. Meanwhile, my company was spending a fortune on contract security personnel and CCTV, and the Country Manager was contemplating the installation of covert surveillance and even planting workplace spies – a tactic that we consider to be extreme and only acceptable in extreme circumstances – without any rational appraisal of the risk or any reason to believe such methods and tactics would yield positive results. I needed to find a way of getting behind this to justify any investment in time and resources – we needed to know whether the problem was 'real' or a barrage of false allegations that disgruntled customers or others were trying to weaponise. This was, therefore, a case that demanded some form of quantitative data to help communicate the problem.

This need for numbers evokes the quantitative risk assessment approaches that I may have appeared to disparage in my literature review. However, I didn't believe that it would be possible to 'quantify' the problem, but I did think it would be useful to have some measure to facilitate discussion with and maintain the attention of budget holders, should some investment become necessary.

I began with a criminological analysis of the anecdotal evidence I was able to gather from colleagues, security contractors and local law enforcement officials, as well as incident reports and observations of customer-employee interactions. My initial analysis produced a typology of the combined threats of customer bribery and employee corruption in which they appeared to take

three broad forms, which I termed *tipping*, *bribery* and *extortion*. All appeared to be motivated by a combination of longstanding convention and expense avoidance by customers, and by financial gain on the part of the employees.

Tipping seemed to be the most common type of illicit practice and that most likely to yield a 'quick win' positive effect if we could put a stop to it. Tipping occurs when the customer leaves a small amount of cash in the vehicle ash-tray or similar location in the car as a gift for the vehicle inspector to keep. I interviewed several customers in various locations who were caught doing this, some of whom were driving relatively new vehicles that would almost certainly past the test first time. Asked why they had done so, they typically responded with a comment such as 'it's my pleasure' or 'just saying thank you', although a few expressed the belief that the inspector would find a way to fail their car if no tip was found. This kind of activity persisted in those test centres that were able to segregate customers from vehicle inspectors, so there was no way the customer could ask for a special service. Tipping appeared to be a legacy convention from earlier times that did not necessarily require or imply any corruption of the service offered. Although forbidden, it is in some ways similar to the tipping of restaurant or bar staff. However, it could encourage inspectors to relax some of the discretionary rules. It could also cause resentment if the vehicle of someone who has left a tip fails to pass.

Bribery is the next most common type of transaction. This occurs when the customer offers cash to a test centre in return for non-standard service. This typically requires the inspector to turn a blind eye to vehicle failings, which may range from relatively trivial to very serious – especially if heavy goods, public transport or fleet vehicles are involved. It either requires a direct interaction between the customer and the employee, which may take place away from the test centre location, or the involvement of an intermediary, such as one of the insurance vendors.

Providing invaluable technical insights, the technical governance specialist demonstrated how various tests could be manipulated at will. These ranged from using simple techniques like standing on the hose used to measure vehicle emissions to restrict the exhaust flow, to programming analytical computers to allow performance results from a new vehicle to be associated with an older model that would otherwise fail.

The third type of illicit transaction my analysis identified is extortion. This occurs when the employee either requests or demands an illicit payment from the customer to ensure the vehicle passes the test. This can occur regardless of whether or not any faults are detected in the vehicle.

The technical governance specialist and myself worked through the system from beginning to end at each location, accompanied when possible by the Country Manager, the Business Operations Manager and the Branch Manager. I will cover each process in turn but will limit the discussion to the risk of bribery and corruption.

Pre-arrival and greeting

The TV documentary that sparked my involvement alleged that customers faced waiting times of up to three hours prior to the commencement of testing. Their report helped perpetuate a folklore that delays are caused by deliberate 'go-slows' by 'corrupt' employees and managers. This narrative suggests that various forms of illicit additional payments are necessary to ensure a pass result.

I discovered that archaic legacy arrangements require almost every vehicle owner to renew their vehicle tax in the month of December. However, private vehicle ownership has grown exponentially since democratisation so the government introduced a half-year renewal point in June. I took the photograph on the left during a June visit and it shows vehicles waiting to enter TC1. The bottom photograph is a screen grab showing the same scene from a different angle, taken during the peak period for vehicle testing.

A collective risk perception – fuelled by heritage culture, bad planning, poor communication and other inputs – is likely to be a causal factor in the incidence of bribery and corruption. People hear rumours that the delays are caused by corruption, so they decide to offer illicit payments to manage the risk. If one employee accepts a payment, it confirms the rumour, and if they don't accept, some will say the offer was too low.

In addition, analysis of past records by the technical governance specialist found that the primary causes of most re-tests were a product of customer non-compliance with rules and standards with which they needed to comply before arriving at the test centre. The country neither enjoys or suffers a rule-based culture, so compliance is probably going to take several generations to become 'normal'. Nevertheless, regulations specify some important pre-requisites for testing that, if enforced, may require customers to be turned away.

For example, all vehicles must have a valid road tax, yet security personnel who administer admission to the centre are not instructed to check if this documentation is present and correct – an omission that allows frustration into the system when it could be diverted. All the test centres visited have vehicle tax offices nearby, so it is common for customers to park up either in the testing centre queue or on its parking area, then purchase their tax before booking their vehicle in for test. This elongates their visit, uses up valuable parking space, causes congestion and disrupts the flow of business through the testing centre.

On arrival at the entrance, contract guards admit vehicles if there is parking space available and control access at the gate if there is not. There is a risk at this point that customers may respond to rumours and their own frustrations and attempt to bribe the security guard to jump the queue – even though guards have no influence on how the booked-in queue is managed. Further, if a guard

is colluding on any organised scams with inspectors or other employees, then this initial contact is a good point to propose illicit activity.

Parking

The current system requires the customer to park their vehicle, remove any items of value, then to attend the Reception to follow the 'book-in and pay' procedure. It is at this point when the customer may leave a tip (typically around £10-15) somewhere in the vehicle where the inspector is likely to find it during the 'test' process (see below).

Insufficient management of the parking process also provided opportunities for bribery. This involves different operational dynamics to tipping because it requires some form of negotiation between the various parties, so opportunities for contact between customers and inspectors are very significant. Security personnel are instructed to minimise such contact, but their ability to do so is severely limited by the physical design of the test centre, as well as its social context. As mentioned earlier, many drivers leave their vehicle parked alongside those waiting to be tested while they visit the nearby Ministry of Transport offices to purchase their road tax. It is at this point when managers believed customers are likely to be propositioned about 'fixing' the test by insurance sales people from the kiosks. In addition, inspectors can be observed walking around the car park at this point, and it is possible for a newly arrived customer to talk to them. Some inspectors were seen to share a warm embrace with family members or friends, who were having their vehicles tested. This co-mingling presents an opportunity for customers to offer bribes if they know or believe their vehicle is defective before testing.

Book-in & pay

This process involves the customer presenting the required documentation, paying for the required service and submitting their vehicle keys to the cashier.

Payment is exclusively by cash and this is a 'hot spot' for the payment of illicit incentives which the cashier may collect on behalf of inspectors who are inaccessible to the customer. This requires collusion between at least two parties but probably more, and it is likely to increase if increased restrictions on customer-inspector contact are enforced, e.g. by physical barriers.

After accepting payment, the cashier places the vehicle keys and any associated documents to one side – sometimes in a plastic folder – for collection by the inspector. It is crucial to the disruption of bribery that inspectors cannot choose which vehicles to test.

Test

After collecting the vehicle keys, inspectors proceed to the parking area to locate the car, which they are instructed to inspect for tips and any other contents that violate test centre policies. One day, during about 20 minutes of overt observations on the TC1 parking bay, inspectors engaged in this process reported to me five separate incidents of tips being left in vehicles in a manner similar to that shown in the photograph. There is no reason to believe this was due to any exceptional behaviour by customers on that day, although the fact it was reported was almost certainly due to my presence with the Country Manager and others. It is at this point that I recognised an opportunity to build a new procedure into this process to gather data on the frequency and amount of tipping that goes on. I'll explain this and the results it achieved in the summary.

If the inspector can identify the customer at this point, there is an opportunity here for *extortion*. Whereas bribery is customer-driven, *extortion* is driven by the inspector or supervisor. In its most advanced and harmful form, extortion may involve internal collusion between cashiers, supervisors and even managers, and external collusion with insurance sales personnel and government officials. As with the other threats discussed, there is no objective information on how widespread extortion is although in theory it is more likely to be reported by customers. A complaints/whistle-blowing telephone number is well-publicised within the testing centres, although local management say that customers use it only to complain about waiting times and rarely provide meaningful information.

TC1 attempts to separate inspectors from customers by use of a low plastic barrier separating the parking area from the customer waiting area. However, interactions between customers and inspectors were observed during the visits and these are an ideal opportunity for parties to engage in illicit transactions. No such barrier was present in other locations, and it is left to contract security personnel to 'police' interactions. This is likely to be highly ineffective and a more rigorous system is needed to maintain this separation.

The problem continues inside the testing areas of some of the centres, where welded wire-mesh fencing is used instead of glazing to allow customers to observe the testing process (see photo, taken at TC2). Unless vigorously supervised, this kind of fencing not only allows verbal interaction, but also the passing of cash.

The best point to consider and address the need for separation is at the building design stage, which should incorporate physical barriers into the layout. However, it is possible to re-engineer or 'retro-fit' most locations to better maintain security.

Recommendation

It is difficult to know the size of a bribery and corruption problem because it is purposefully hidden. This problem is exacerbated when the monies paid do not belong to an organised entity that can assess its losses. There is no 'hole' to enable calculation of any missing money and all payments are made willingly, unless there are complaints and evidence of coercion.

I mentioned above that I had an idea when inspectors called out to us about money left in cars. Five notifications in 20 minutes works out at 15 per hour in a car park with the capacity for 50 vehicles which was about three quarters full at that time. If we rounded this to an average of ten per hour for a ten-hour business day and roughly £10 per tip, we have an economy worth around £1000 per day. If all ten inspectors from two shifts were involved, this would work out at £100 tax free bonus per day, compared to a taxable wage of less than £30 per day. Even if we slashed this guesstimated bonus by 50%, it still more than doubles an average employee's pay, and even a 75% cut would come close to matching net wages.

This provides a powerful incentive to accept tips (remember, this analysis doesn't include bribes and extorted money), so how could we incentivise them to report these occurrences and refuse the money?

I proposed a formal bonus scheme that rewarded them for reporting the cash they found. This included a procedure whereby the inspector would summon a security guard as a witness and the owner of the vehicle. They would hand the customer a document reminding them of the anti-bribery policy and would ask them to remove the money. The process would be designed to cause some inconvenience, such as a delay, and the inspector would complete a form with the vehicle registration number and other details. The completed form would be registered, providing anti-bribery performance data for that individual employee and also for the shift and the test centre. Anyone performing below the average could be targeted for closer scrutiny and re-training, or even surveillance if there were acceptable grounds for doing so.

The scheme was accepted and sums equivalent to around £75,000 were handed back to customers in the first two months of operation. Several employees resigned and others were subjected to disciplinary actions. This would not have been possible without the BPSA.

However, over time, these returns diminished and evidence emerged that some employees simply regarded this as a tax, which they colluded in maintaining at a certain level while pocketing the rest. Nevertheless, the operation provided at least some indication of the extent of the problem. These illicit transactions present various risks to the company, as well as to the general public. While tipping may appear relatively innocent, it undermines the integrity of the testing process and help perpetuate a view of the business as corruption-driven. Various media reports cited negative comments from customers, so the risk here is reputational damage.

Bribery is likely to present the most serious risk because it is customer-driven, likely to be accepted and less likely to be reported. Customers who engage in this activity may include haulage contractors, taxi companies or bus companies who have a huge financial incentive to keep their vehicles on the road, regardless of their condition. The risks to road safety cannot be overstated.

Extortion is also serious, although its probability may be reduced because it at least provides some opportunity for offended customers to report the incident, which increases the chances of detection.

Applying Mars' animal typology (Figure 3, page 40), the business seemed to suffer from employees operating as either 'wolves' or 'vultures', depending on the size of the location. TC1, with its multi-lane facilities and the possibility of managers unpredictably rotating staff to frustrate planned processing of unroadworthy vehicles, requires a disciplined team-oriented 'wolfpack' approach. This is to ensure illicit services are delivered efficiently and without delay to customers. The smaller test centres need at least a loose team to reduce the risk of illegal activity being reported, but the activity itself is more likely to be carried out by individuals. There was also a risk of 'donkeys' operating in the book-in and payment area, who could easily provide information about cash handling procedures to external threat agents planning a robbery.

Sensemaking summary

How does something come to be a security risk event in this business?

In this case, a scandal presented on national television triggered some actions but it didn't provide any information about the likely extent of the problem. Further investigation established three forms of corruption that varied in frequency and impact and the BPSA helped identify a means of measuring them.

What impact would it have?

Tipping is forbidden, undermines the quality of service and could have negative impacts on inspector behaviour and customer relations. Bribery could result in catastrophic harm resulting from an unsafe vehicle causing a fatality after being defined as safe by a corrupt employee. This would have severe business and employment consequences, in addition to the tragedy of any casualties. Extortion would be more likely to be reported, but this would have severe reputational consequences for the company – especially if reported to a third party, such as a newspaper.

What can we do about it?

The BPSA found opportunities both for relevant data gathering and for implementing an 'integrity performance' measure for employees and locations. This required them to self-report any cash tips left in vehicles, thereby providing an indication of the value of the informal economy and the frequency and value of individual inspector's reports. This was implemented and achieved its objectives for several months, until employees found a means of effectively defeating the control.

CASE STUDY 3: Plant and laboratory operations in a Latin American gold mine

This case study is of my first application of BPSA in a commercial context and concerns a project undertaken for an external customer of the Minerals business. As I have a previous background in security consulting, I am available to any of my company's businesses to provide security advice and expertise to external customers subject to availability. In this project, I had the opportunity to work with several mining specialists who had expertise in plant and laboratory operations. We collaborated on a detailed proposal and won the tender because none of the competitors were able to offer the security component without contracting out.

Setting and context

The project was an ambitious undertaking because of the complexity of plant and laboratory operations in such large facilities, the high-risk nature of the surrounding territory, which is notorious for its lawlessness, and also the challenge of establishing a collaborative approach between a diversity of disciplines coming together for the first time. None of the other experts had any training in security risk management and, although I had undertaken security projects on several mines in Latin America, Africa and the Far East, my knowledge of technical processes was rudimentary. I therefore had to get an overview of everything that happens to excavated material after it reaches the surface and begins its journey towards becoming gold and silver bullion.

From a security risk management perspective, the job was a great opportunity for my project because of the focus on *process* and *insider* threats. Mines such as this have highly defensible borders that are protected by paramilitary security forces authorised to use lethal force. Although the organised criminal groups that present the external threat do have kinetic capabilities, they would be more likely to target product in transit (was beyond our scope because it was contracted out) rather than risk attacking the mine itself.

Before deployment, we assembled the project team in a neighbouring country to make an operational plan. As they had not worked with me before, the other members asked me to explain my approach and what I would be looking for, so I gave a short presentation on the core concepts in security risk management and presented them with BPSA. They then agreed to adopt it as the core methodology for the whole project, as they felt it was just as appropriate for their technical and quality evaluations as for security. However, the final report had to be structured with different chapters for each area of expertise, so I will only present the security risk management perspective in this case study.

On arrival at the mine, we split into two teams: *plant* and *laboratory.* I worked for two days with the plant team which allowed me to follow the various processes from excavation to the point of bullion production and collection by contract security. I then spent time with the laboratory experts tracking the path of samples which were sent there for analysis from various processes I had observed in the plant system.

This case study is presented in its original form to preserve the authenticity of how I communicate my findings to my company. However, it has been redacted, edited and annotated to fit the purposes of my project.

Figure 14 on the following page shows a system map created in Microsoft Visio superimposed on an architectural drawing of the main Plant and Laboratory parts of the mine. However, this example doesn't show process ownership, because it was impossible to map that onto the site plan. The processes flow broadly clockwise from the top left and are shown in purple rectangles. Samples and their flow to the Laboratory for analysis are shown in orange. Risks are highlighted in red and at the points A-E, while commentary on existing controls is shown in dark blue. Imposing the processes on to the drawing helps provide a sense of the spatial relationships involved. This is important, because materials can be intercepted more easily if distances are greater.

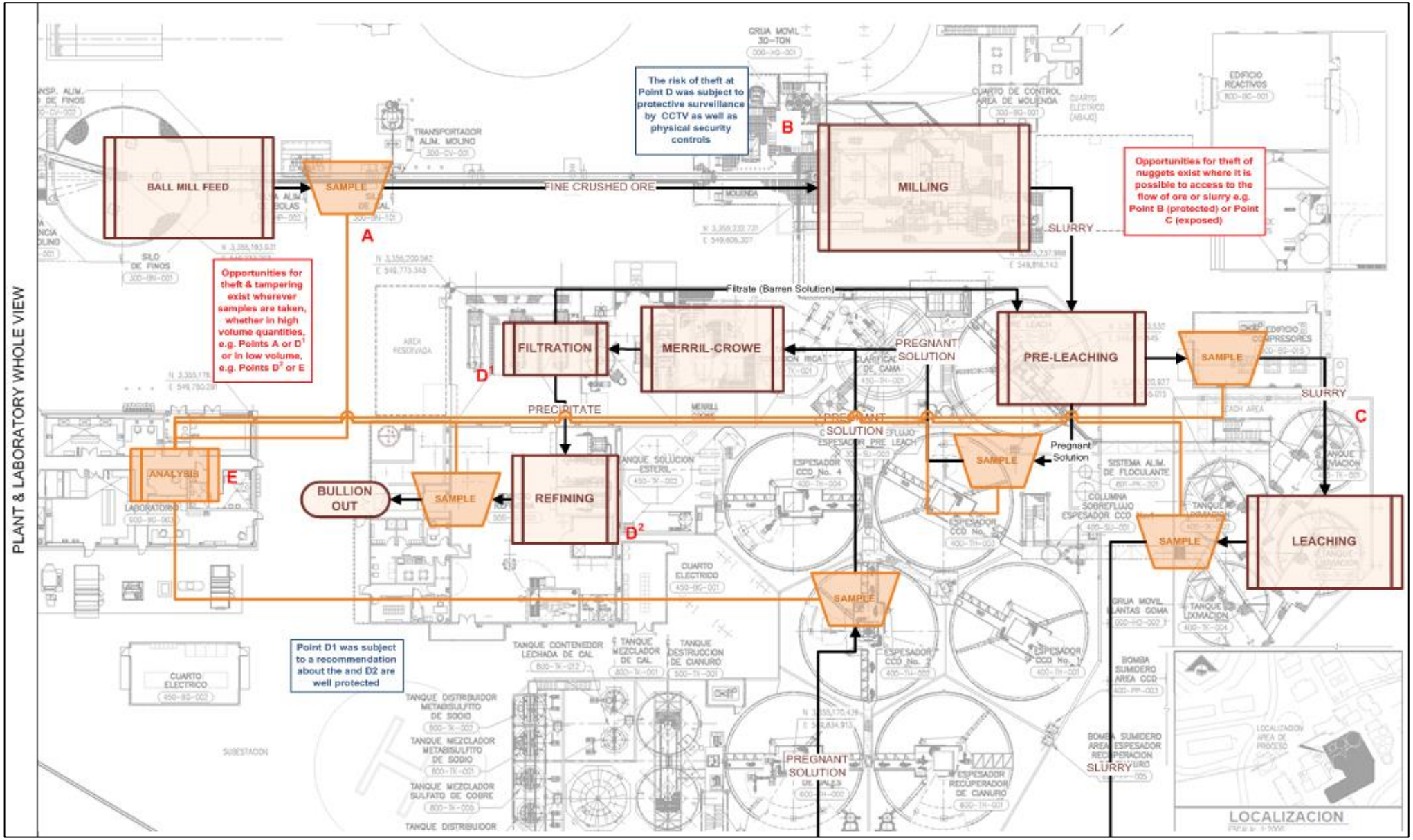


Figure 14: BPSA Superimposed on Architectural Drawing

Although access to the wider area is restricted by layered fencing, vehicle check-points and searches of visitors and employees by security personnel, the outside areas within the perimeters are relatively open and it is possible to move quite freely between them once inside.

Access to high risk areas, such as the Refinery (Points D^1 and D^2) and the Laboratory (Point E) are much more strictly controlled with armed guard patrols and additional access control technology applied to doors in the case of the lab, and a very rigorous, multi-level access control procedure for the Refinery.

However, there are few physical impediments to prevent someone moving, for example, from Point A to Point B, once they are on site, although such movements would be monitored by CCTV and would certainly produce a response if identified as a concern by monitoring personnel. The fact that all cameras are recorded would also facilitate future investigations if evidence of suspicious activity became known after the fact.

Broadly, the approach to security in these areas was appropriate: commensurate with the risks and supportive of the working processes. However, there were opportunities for improvement.

To understand these in greater depth, I adopted an offender perspective based on the availability of attractive opportunities for theft, with a particular focus on the mine's mineral products (i.e. not tools or high value consumables, which could also be vulnerable).

The four targets of opportunity are, in order of perceived attractiveness:

- Doré bars (see below for an explanation)
- Precious metal shavings
- Precious metal nuggets
- Precipitate

The following sections will consider the exposure of each of these in turn.

Doré bars

Doré Bars are partly pure alloys of gold and silver that are produced in the mine's Refinery after filtration and smelting. Molten metal is poured into an iron mould, allowed to solidify then cooled and cleaned of slag material. The product is then stamped and weighed before small samples are taken and the bar is stored in the Refinery vault. Comprising around 60% silver and 40% gold, bars typically weigh around 20kg and are easily transportable by an individual of average strength. Examples observed during the audit were estimated to be worth around US$1.6 million each based on contemporary gold prices. Doré Bars are an extremely high-value and portable target that are easily converted into cash, so they are very attractive to thieves and the processes that produce them must be extremely well-protected.

Figure 15: Production & storage of Doré bars

Figure 15 shows the Doré production process. Clockwise from top left: smelting, cleaning, temporary storage in the small safe, medium-term storage in the vault wherein each bar is stamped with a unique identifier and the mine's code. The vault requires two combination-holders to be present: the Refinery Supervisor and a representative of the Control Team who attends specifically for this purpose, and to witness the relevant procedures. During the visit, the process was observed to be subject to intense scrutiny, both by the personnel present and by CCTV.

The security of Doré bars is highly dependent on the design and operation of the Refinery. This has a good basic design, but in its original form (prior to recent changes to the security arrangements) it lacked sufficient consideration of the security risks emerging from internal threats (i.e. from Refinery personnel) and collusion with outsiders with access to the perimeter of the building shell.

Figure 16 shows the original architectural drawing of the refinery, with new security measures shown in dark blue and the entry route shown in red.

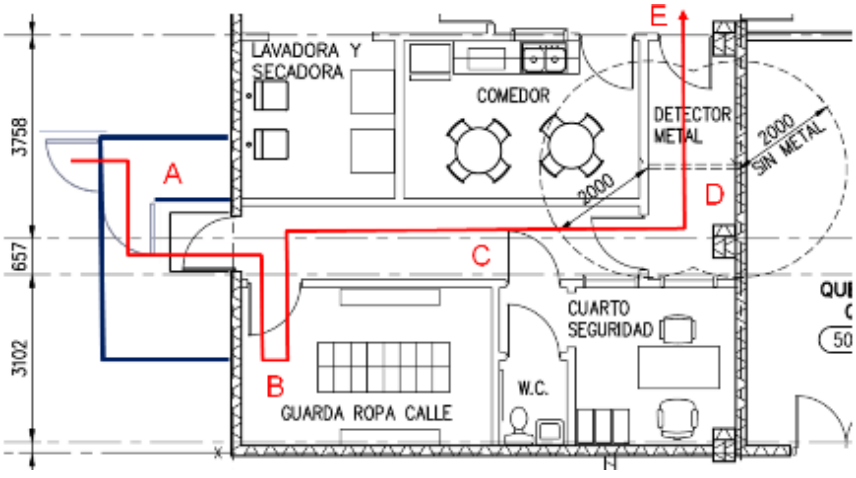


Figure 16: Plan view of the access control measures to enter the Refinery

(Glossary: *Guarda Ropa*: changing room; *Cuarto Seguridad*: security room; *Comedor*: dining room; *Lavadora y secadora*: laundry and tumble dryer; *Sin Metal*: no metal allowed)

Point A of this plan shows the entrance point, which consists of two locked gates operated by two armed security officers (Figure 17). Access is provided solely by prior announcement and each gate is unlocked only after the previous access point is secured.

Figure 17: Refinery access control

- Access is also monitored by CCTV.
- The experience of two entries into the Refinery demonstrated a consistent level of discipline by security personnel.
- However, the risk of prior announcement given under duress should be considered.
- It was recommended to require written and signed authorisation for access to the Refinery.

Following admission into the Refinery building, visitors and employees are required at Point B to undress to underclothes and shirt, followed by a non-invasive physical search and scanning with a metal detector at Point C.

- Searching is monitored by CCTV.
- Observation of several searches indicated a ‘standard’ approach to body searches, involving the same search actions every time. Such routine activity creates opportunities to evade detection. For example, the requirement to show the sole of each foot without removing socks allows the concealment of non-metallic items next to the skin.
- It was recommended to train security personnel to vary search techniques to introduce an element of unpredictability into the procedure.

Point D represents a metal detection process that seems to be effective and it was to the credit of security personnel that they spotted important detail, such as the wearing of gold jewellery which had to be removed. This process was also monitored by CCTV and takes place with both doors locked.

Point E represents completion of the access control procedures, at which point visitors acquire disposable overalls and employees put on their regular working attire, prior to entering the main operational area where filtration and smelting take place. NB: working attire is laundered only within the facility and never leaves until destruction and disposable overalls are either reused or burnt within the facility.

No tools are allowed to be taken in or out of the Refinery. According to previous studies of Refinery security, this is consistent with established principles of best practice:

> The most effective method of preventing a person from removing something from the secured area is to prevent him/her from taking anything in, in the first place. It is therefore essential to control the movement of equipment and tools used by contractors and mine employees. Equipment is time consuming to inspect and lends itself to be used as smuggling containers.
>
> Coetzee & Horn (2006): 51

However, it was observed that such restrictions were not previously in place and employees exploited the opportunity by removing valuable scrap material in oil cans and similar receptacles.

- It was recommended to ensure lessons learnt from this mine and those of other companies are comprehensively implemented in all locations

Figure 18: Refinery Emergency Exit

Some theoretical opportunities for theft do exist, but these could only be exploited for thefts of small quantities of material. For example, Figure 18 shows three views of the only push-bar emergency exit from the Refinery. The image on the top right shows and exposed gap beneath the door as seen from inside, while the other two images provide the external view. This exit leads into an external area that was designated ‘restricted’ in the original plans, possibly to be protected by a fence similar to that that has been added to protect the Refinery entrance.

Although the area is protected by CCTV, it would be possible for some to push small quantities of material through the door for collection later or by an accomplice. A similar gap was observed underneath the rolling blinds and external area next to the loading bay from where the Doré is collected prior to leaving the site.

It was recommended to ensure all doors and windows are fully controlled to ensure both safety and security

During a follow-up visit to the Refinery after smelting had finished, the small temporary safe by the vault was observed to be open and unattended with the key in the lock (see Figure 19, top left). The safe was empty, but the key could be used to create a replica or even lost, causing disruption to the safe’s role in the security of Doré production.

Figure 19: Post-smelting issues

Figure 19 also shows some of the slag left over from the smelting process. Significant quantities of precious metals remain in this material, so it is also vulnerable to theft and re-processing off-site. Best practice is to ensure its secure disposal by re-cycling it into an appropriate point in the plant processes. However, Plant and laboratory experts found that doing this might create a false impression that theft is taking place. Recycling high value scrap from the refinery by putting it back into the preparation processes to capture any remaining precious metals second time around results in false readings at various points where the gold content is made to look higher than it is. This needs to be factored into the monitoring process, or an alternative means of processing the scrap must be found.

At present, the Refinery floor is very untidy with an abundance of this material waiting to be crushed. A new milling machine is on order, which will facilitate the processing of this material within the Refinery.

Of course, theft of Doré from within the Refinery environment can be achieved by stealth or by force, the latter presenting the highest rewards and the greatest risks for the offender. The best time to attempt such an attack would be during the collection of bars for transport off-site. This is performed by a contract guarding company who transport the bars under armed escort to the nearest airport, approximately three hours drive away (see Figure 20).

To attempt an assault on the Refinery at any other time would present a huge challenge, because of the time it would take to penetrate its extensive physical security and the high risk of armed intervention before the attack could be completed. Similarly, an attack on the bullion during the collection process would also be very difficult, and anyone who could seriously contemplate such a thing would quickly conclude that it would be far easier and more likely to be successful to attack the security transport vehicle on the open road.

This is no argument for complacency and even less for reducing the level of security afforded to the Refinery and the collection of bullion, as it is essential to maintain the intelligent conclusion that any attack seeking to use overwhelming force would be a waste of resources.

Figure 20: Armed security collecting Doré bars

It was recommended to maintain existing levels of physical security for the Refinery and the collection of bullion and continue to ensure all risks are transferred to the security transport company on collection.

Recent improvements to the access and egress control systems of the Refinery reduce the opportunities for theft and increase the risks of detection for offenders. Some minor loopholes – such as the spacing under external doors and the repetitive nature of body searches – need to be closed off, and new mill is needed to help maintain order and limit access to potentially valuable scrap. Discipline needs to be maintained, as shown by the key being left in the temporary safe, in order to demonstrate a high level of security awareness and to promote a positive security culture.

The threat of an attack by force is unlikely and existing security arrangements are sufficient to ensure that this remains so in the current 'risk climate' of the region. Anyone capable of seriously mounting such an attack would probably opt to attack the bullion in convoy, rather than risk a prolonged and dangerous affray on the mine site.

Summary of Recommendations

- Require written and signed authorisation for access to the Refinery
- Train security personnel to vary search techniques to introduce an element of unpredictability into the procedure
- Ensure lessons learnt from this mine and those of other companies are comprehensively implemented in all locations
- Ensure all doors and windows are fully controlled to ensure both safety and security
- Continue to maintain existing levels of physical security for the Refinery and the collection of bullion and ensure all risks are transferred to the security transport company on collection.

Precious Metal Shavings

After the Doré bars are forged, cleaned and stamped, precious metal shavings are extracted from each one and sent to the Laboratory as samples for testing. Figure 21 shows the relevant processes clockwise from top left. After the bar is weighed, a small hole is drilled and the resulting shavings are extracted, weighed and placed in a transparent plastic bag which is then numbered and sealed. Each bar is then re-weighed to reconcile the tiny amount of material that has been removed and the results are recorded in longhand. The shavings are then placed in a locked box which is then transported to the lab by armed security personnel.

The entire process is witnessed by a member of the control team and is observed and recorded by CCTV.

Figure 21: Precious Metal Shavings Extraction & Handling

On arrival at the Laboratory, the samples are weighed by Technicians and the results confirmed. This process is monitored by CCTV and witnessed by a security officer, who also signs the relevant paper records. The samples are then kept in a small safe and accessed in accordance with Laboratory procedures for analysis.

From the offender perspective, theft of precious metal shavings must be a sustainable proposition that can be repeated over time. This is because the value of what could be removed from the registered and recorded volume of samples is very small and of too little value to justify the risk. For the reason, the best defence against theft is a rigorous sample management system with the overall policy framework of a well-run Laboratory.

Cumulative batches of samples were returned to the Refinery that could not be cross-referenced back to the original individual samples. This also creates opportunities for small amounts of material to be skimmed from the aggregated batch.

Further, current practice makes use of unnumbered, loose leaf records that are handwritten. This weakens the security and control system as it creates opportunities for minor alterations to records to facilitate the theft of small quantities of materials.

It was recommended to either make fuller use of the laboratory information management (LIMS) system to ensure sample details are recorded by the Laboratory hardware OR initiate a more rigorous system of manual recording that can be subject to peer review

In addition to apparent weaknesses in the Laboratory management system, some opportunities for unauthorised access to or egress from the building shell were identified. This was in spite of the fact that a good electronic access control system is in place, and that one armed guard patrols the outer shell, while a static guard is placed in the main corridor inside.

Figure 22 (left) shows the guard patrol as viewed from inside the building whereas the image on the right shows the same two doors left open and unattended, while the guard is elsewhere. This is not a critical issue in terms of gaining access, although it does provide an opportunity. Rather, it allows someone from within the building to pass something outside – very much like the emergency door problems found in the Refinery.

Figure 22: Laboratory Building Shell Security

It was recommended to either provide an alternative form of ventilation to remove the need to open the doors, or enclose the nearby outside area with a perimeter fence. This would also facilitate external storage of samples.

In summary, the security of precious metal shavings was generally very good, but some opportunities to breach the system do exist. An overall recommendation to encourage greater dialogue between the mine's security management and those responsible for the technical governance of the relevant processes. This would ensure a tighter net involving physical security, human and technical surveillance and Laboratory procedures and management.

Precious Metal Nuggets

Precious metal nuggets are lumps of precious metal found ready-formed in the earth. They are usually small and easily concealed about the person and easily exchanged for cash.

There are certain points in the plant production system where nuggets are more likely to become accessible.

Figure 23: Opportunities for Theft of Nuggets

Figure 23 shows two pictures (left and centre) of the crusher area that precedes the ore's pathway to the mill and one picture of the exposed cyclone cluster that follows milling. Nuggets can be found at these two points, so the crusher area is seen to be protected by several CCTV cameras and chain link fencing. However, the central picture shows that the chain link roof of this area was severely damaged, enabling easy human access. It was not possible to determine if this had occurred by accident or deliberately, but it provides an opportunity for illicit activity that should be closed.

It was recommended to ensure physical security protections are properly maintained and promptly repaired

The cyclone cluster shown in the right hand photograph is insufficiently protected, as there is no CCTV and no physical barrier to prevent access to the flow of mineral-rich liquid. This provides an opportunity to place a robust basket in the flow, in the hope of capturing some nuggets that can then be stolen.

It was recommended to monitor the cyclone cluster with CCTV and enclose it with either chain link fencing or a similar material that allows maintenance but discourages opportunistic 'fishing' for nuggets

Stealing nuggets is an opportunistic crime that an individual may seek to exploit but that does not lend itself to organised or planned commission. However, it is important to maintain the honesty of employees by removing temptations and ensuring the product system is fully protected.

Precious Metal Precipitate

Precious metal precipitate is produced within the Refinery following filtration, as shown in Figure 24 and also at Point D[1] in Figure 14 on page 90.

Precipitate is rich in the precious metals that refining will extract into Doré. However, it remains a bulky material which poses a challenge to anyone thinking of stealing it. As with precious metal shavings, it can be stolen in small quantities over time, but this requires a sustainable theft model requiring repetitive behaviour and exposure to the risk of detection. It can also be stolen in bulk, perhaps taking advantage of a cleaning procedure or similar event that opens the Refinery to allow removal of accumulated materials. Existing countermeasures include physical security and access control to the Refinery and CCTV monitoring of the filtration area.

Figure 24: Filtration & Precipitate Production

Sensemaking summary

How does something come to be a security risk event in this business?

Precious metal mines produce high value materials that are easy to convert into cash if controls are evaded. The primary risks identified derived from insider threats, primarily by employees, exploiting small opportunities for small scale theft over a period of time. All the more serious threats were very well-covered by existing arrangements.

What impact would it have?

Apart from the obvious direct losses, an employee theft problem results in drastic loss of market confidence in mines, most of which rely on outside investment. In certain circumstances, this could lead to mine closure and massive losses in investment and employment.

What can we do about it?

Mine security was generally very good, but minor lapses provide opportunities that intelligent offenders would be quick to exploit. Gaps under doors, apparently trivial breaches of security protocol like leaving doors and windows open for ventilation, and similar issues were found.

CASE STUDY 4: Textiles laboratory in North Africa

This case study is based on a security risk assessment that was requested by the Country Manager after discovering that a customer services manager in the Affiliate's textiles laboratory had been altering test results in favour of a client. This is a serious breach of the company's Code of Integrity which may have resulted in sub-standard textile products being approved for shipment from factories in the country to their customers in Europe, North America and other parts of the world.

The business of a laboratory of this kind is to test products – in this case textiles, but in other location it could be toys, soft furnishings or 'hard lines', such as garden furniture and tools – to ensure they conform with any applicable legal standards (e.g. for fire safety or toxicity) as well as the quality standards of the buyer. *Buyers* are usually large retailers in Europe or the Americas, but they could also be importers or traders. My company's *customers* are the manufacturers or producers of the goods. This produces a rather unfortunate arrangement wherein my company's customer pays it to test products to the standards of their customer (i.e. the buyer), so we, in effect, represent the interests of the buyer – yet we don't get paid by them: we get paid by the people who whose products we may fail. The operating principle is that the manufacturer doesn't want sub-standard products to go to market, because they will tarnish their reputation and may put them in breach of contract. However, international trade is not so simple and the resulting dynamics result in the employees of testing companies being subject to bribery and other incentives to manipulate samples, processes, results and reports to suit illicit interests.

In the case that resulted in my involvement, the customer services manager was dismissed and the company lodged a criminal complaint with the police. However, police investigators wanted to broaden the enquiry to interview other company customers who were not involved in the case, in order to gather comparative evidence about 'normal' practices. This is a good example, further to my observations on public and private justice systems in the literature review, of a police investigation making matters worse for a business, in this case by disclosing its internal problems to the outside world. This would certainly spark rumours and cause further reputational damage, so the criminal case was dropped. However, the newly appointed Country Manager wanted to be sure that the systems and processes in place were not vulnerable to a repeat attack. BPSA was, by this time, my company's approach of choice, so I was asked to lead an in-depth review of the laboratory's business.

Although I had started to refer to the *McKinsey 7-s* framework in some previous cases, this was the first time it took centre stage in the analytical framework and report structure. This is because the BPSA approach was starting to indicate that the problems identified and the solutions advised more explicitly concern management and organisational aspects as causal or contributory factors. Building on the experience of other disciplines accepting the approach as an analytical framework in the previous case study, BPSA had evolved into a more holistic tool that could identify, quality, HR and other issues, in addition to security risk management.

The analysis begins with *shared values*, as these should govern everything that follows. The process map and systems analysis is embedded under the 'systems' heading in a few pages. This process map also shows process ownership, which is now standard BPSA practice.

As with the previous case study, the following text is from the original report to business, but edited, redacted and annotated for its purpose here.

Shared Values

Shared values are about what the organisation stands for and what it is trying to achieve. This aspect is particularly relevant to this lab as there were indications that some employees were somehow disconnected from its purpose and their role in the 'big picture'. Interviews with personnel

and accounts of their comportment by managers suggested that rivalries and informal associations between different groups of employees were taking hold of the workplace culture. The dismissal of the former customer service manager and the appointment of a new Country Manager had disturbed the status quo, and there were some talented people who seemed to have been marginalised under the previous leadership that now had an opportunity to flourish.

However, there were concerns about integrity training. The laboratory quality manager confirmed that each new employee receives and signs the Code of Integrity when signing his or her employment contract, but they don't receive the associated integrity training until later. Human Resources, who administer the training should normally send a link to new employees and ask them to complete online training within three months of their commencement, then follow up to check if the employee as successfully performed the test. However, the online training programme for new employees was not currently implemented in this country and this had resulted in an 'integrity gap'.

The most recent face-to-face integrity training session for the laboratory team was held in the early months of the previous year, while the session for the current year was planned for mid-November, leaving a gap of over 18 months which is far too long. Further, it was emphasised to the Country Manager that, to reinforce its importance, the laboratory manager and Business Manager must participate *actively* of integrity training by leading the discussion with real laboratory examples, not just the sample case studies provided by Global Compliance. Good examples can have a real impact on each employee because they bring the issue to life and explain how a breach of integrity could affect them directly.

RECOMMENDATIONS:

- Promote the 'integrity message' with an internal publicity campaign, including integrity posters throughout the laboratory and publication of the Integrity Statement in the Reception area to drive home the message and re-establish an Integrity Culture.
- Ensure the annual Integrity code training is applicable to local issues, especially pertaining to the laboratory and known risks and with a particular focus on consumer safety. Integrity e-learning for new employees must be mandatory.
- Seek out and recognise actions that reinforce integrity, such as the reporting and recording of unacceptable requests by customers or others.

Strategy

The strategic challenge for the business in this country is increasing growth and market share while maintaining the shared values described above. According to local management, the business is under constant pressure from customers to approve products that do not comply with buyer standards. Such pressure can be applied to individual employees who may be subject to bribery or coercion to subvert processes, data and reports.

Criminologically, this is an offender probing our defences for opportunities. These attempts must be resisted and the strategy for growth must incorporate the shared values to prevent future claims

against our company. This begins with a process of risk assessment that identifies threats to operational processes and reputation, most notably customer attempts to influence operations.

RECOMMENDATIONS:

- Strategic planning should ensure that risk management is fully integrated into every aspect of business design, led by senior management and incorporated into all role descriptions.

Structure

The structure of the laboratory comprises Reception, Customer Service, Preparation, Chemical Laboratory & Physical Laboratory divisions, supported by Back Office and Quality Management functions.

With the appointment of the new Country Manager and a new Business Manager, there is an opportunity to strengthen and enhance the shared values of the laboratory team with positive leadership. The Business Manager seems to be well placed to instil a new lab organisation, a new style of management and to underline the need for strong integrity values. However, he cannot do that alone and needs to rely on his team and to be able to trust and delegate to the relevant managers.

We noticed that the Business Manager felt of a lot of pressure from clients and also from the lack of organized structure and put in a lot of hours including weekends in order to organize the laboratory with a system and process which did not yet exist when he joined and which form the basis for the good laboratory practice

The quality manager is junior and needs some coaching but she seems proactive and ready to implement any change to improve the quality of the lab processes. She should be working closely with the laboratory members in order to ensure that she can improve the process continuously and prevent any issues before they arise.

RECOMMENDATIONS:

- The organisational structure should be re-evaluated to ensure clarity in terms of reporting lines and accountabilities. A ‘checks and balances’ process must be established to ensure that every level of laboratory operations is checked by the supervising manager. This must be done frequently and with the goal of reviewing and improving processes and procedures in a collaborative way.
- Team Leaders must regularly audit the performance of individual team members with direct observations of their work. This is an opportunity to provide advice, training and support, as well as supervision, but it must be unpredictable and not subject to any routine.
- The laboratory team must be aware that LIMS system is recording every move on the system and that the tracking leaves an audit trail. The managers must organize session with the team to show this is a way to check a specific job file and to trace if all the tasks have been performed according to the procedure. This is a way to protect the company but also the employee performing the tasks.

Systems

Figure 25 on the following page shows the BPSA for the sample processing system. Processes and links in red indicate the presence of identified security risks. Comments in blue refer to suggested remedial actions.

The system begins with the arrival of a sample at the Laboratory Reception. This is recorded in longhand in a register of samples and the delivery person is issued with a stamped receipt which is returned to the customer. To her credit, the Receptionist demonstrated awareness of the importance of keeping the company stamp secure and keeps it under lock and key after the close of business. Anyone delivering samples out of hours must return during the normal business day to obtain their receipt.

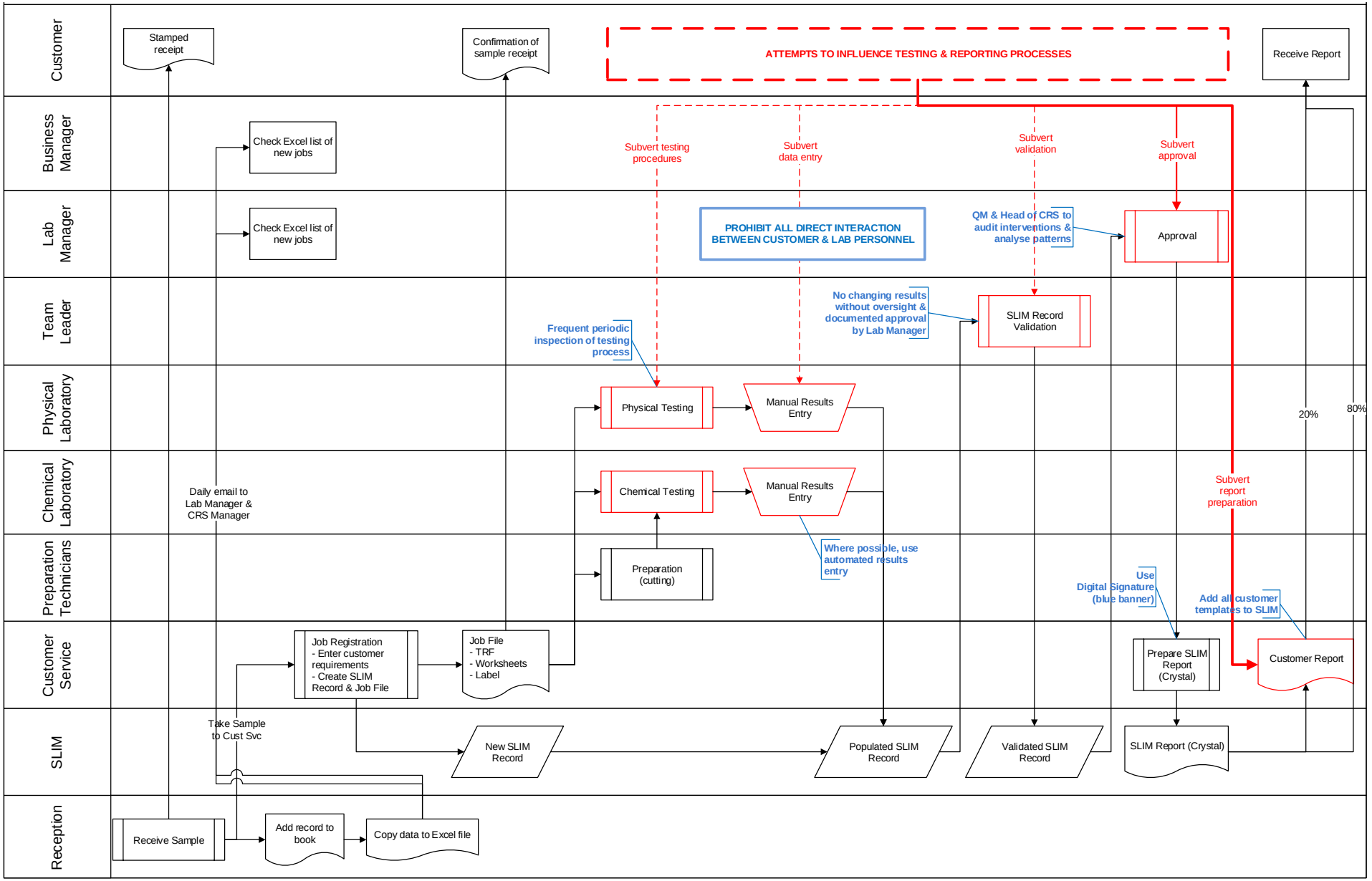


Figure 25: BPSA of the sample processing system of the textiles laboratory

The details recorded in the register are then transferred to a spreadsheet which is shared with the management team at the end of each business day (this gives them an idea of the testing volume of the day). The sample is taken to the Customer Service desk, who create a new LIMS record and a Job File that comprises the sample, a Worksheet and the customer's testing requirements presented on a Testing Request Form (TRF). The TRF is a standard document that is sometimes completed by the client and sent with the sample. If not, the Customer Service team create one based on the customers own documentation.

If the sample is to be subjected to chemical testing, it is then forwarded to the Preparation Technicians who will cut it as specified in the customer requirements. It is then sent to the Chemical Laboratory for testing (e.g. for traces of toxic chemicals). Samples that are to be subjected to Physical Testing (e.g. rubbing or laundering) are transferred directly as any preparation is conducted in the Physical Laboratory.

RECOMMENDATIONS:

- To mitigate risks during the testing processes, it is recommended that the Team Leader, the Lab Manager and the Quality Manager all engage in frequent and random observations of technicians' operations. This should not be done intrusively or for any reason other than quality and integrity management, as creating a climate of fear is always counterproductive.
- The context must remain one of continuous improvement with the aim of establishing and ensuring best practice. Nevertheless, it will also communicate a strong message to technicians and their immediate supervisors that the any wrongdoing is likely to be detected, which will have a deterrent effect.
- Random inspections should be documented and examined for patterns. Care should be taken to rotate them in order not to target any one individual unless their performance justifies it.

Although the laboratory has a LIMS system which in some industries records test data automatically and without human intervention, all the results in this lab are entered manually because many of the tests are visual and require user input. It is at this points that the first risks start to emerge, as there are opportunities to manipulate the testing processes to the customer's advantage (or *dis*advantage, if the motive is sabotage). Interviews with managers and other personnel revealed that customer pressure to produce favourable results is a constant feature of the textiles business and this bears down on most of the operational processes from this point forward.

Possible manipulations include the risk of sample substitution. For this reason, previously tested samples should be subject to access by authorised personnel only, as samples known to have passed may be substituted for samples attached to new jobs with similar materials but known to be of inferior quality. All access to the sample storage should be controlled, monitored and documented

Similarly, there is an opportunity to manipulate results during the data entry process. This is already subject to review by the Team Leader in the process labelled 'LIMS Record Validation'.

The Team Leader has the ability to over-ride results entered by the technicians, which obviously provides an opportunity for changes for illicit reasons.

The previous customer services manager had identified a 'soft spot' for illicit data manipulation. However, had this been secured without detecting his wrongdoing, he would most likely have sought out another opportunity to subvert the system, which could have involved collusion with a colleague or even coercion. Any amendments to a system must consider this risk of *displacement* of an attack from one part to another.

RECOMMENDATIONS:

- This process of over-riding data entry should be subject to a more formal approval procedure that involves the Lab Manager. The Quality Manager should also be notified, as the changes could be indicative of problems in the testing procedure, calibration of equipment and so on.
- All those involved should be made aware of the risk of deliberate manipulation at this point and checking procedures should also be designed to provide assurance that employees are doing their job to the highest integrity standards. Consistent high performance in this regard should be recognised in appraisals.

Next, the validated LIMS record is subject to approval by the Lab Manager. This process should be subject to regular audit by the Quality Manager and Business Manager, as the following step is the preparation of the LIMS Report.

LIMS can produce reports in PDF and Word (RTF). While around 80% of reports are emailed directly to the client, the remainder are sent to Microsoft Word for customer-specified cosmetic modifications. This is currently the point of highest risk in the system, as there are ample opportunities for changing results in the customers' favour. Indeed, it is at this point that the former Customer Services manager seems to have breached security most frequently as output to Word allows *results* to be changed as well as the document's *aesthetic appearance*. Interview with the local team revealed that the Digital Signing solution to secure PDF reports was not implemented in the laboratory.

RECOMMENDATIONS:

- The ability to send documents to Microsoft Word should be restricted if not completely eliminated from the system. If customers require a specific format, their template can be loaded into LIMS which can generate a secure, digitally signed PDF with their specified cosmetic features.
- However, the company should be careful that it does not allow the report to suggest that the customer is authenticated to any recognised testing standard or that the customer has conducted the tests itself.
- PDF outputs should be authenticated with a digital signature as illustrated in the inset. The blue banner provides a highly secure assurance that the document was produced by our company and has not been altered since its emission. Customers and other consumers of

these documents should be educated to look for the banner and NOT to accept as genuine any report without it. This adds real value for customers and also helps align the CRS reports issued with other CRS countries that have been using the digital signature solution for several years.

An additional system that supports business delivery is the communication system, by which customer requests are received, evaluated and acted upon. Security of the communications system is particularly important, given the threat of customer attempts to manipulate the sample testing system described above.

Figure 26 shows how a customer could communicate illicit requirements to a Customer Service operative. If the integrity of this employee is compromised, they are able to act as an internal 'agent' for the customer and issue illicit instructions to test personnel.

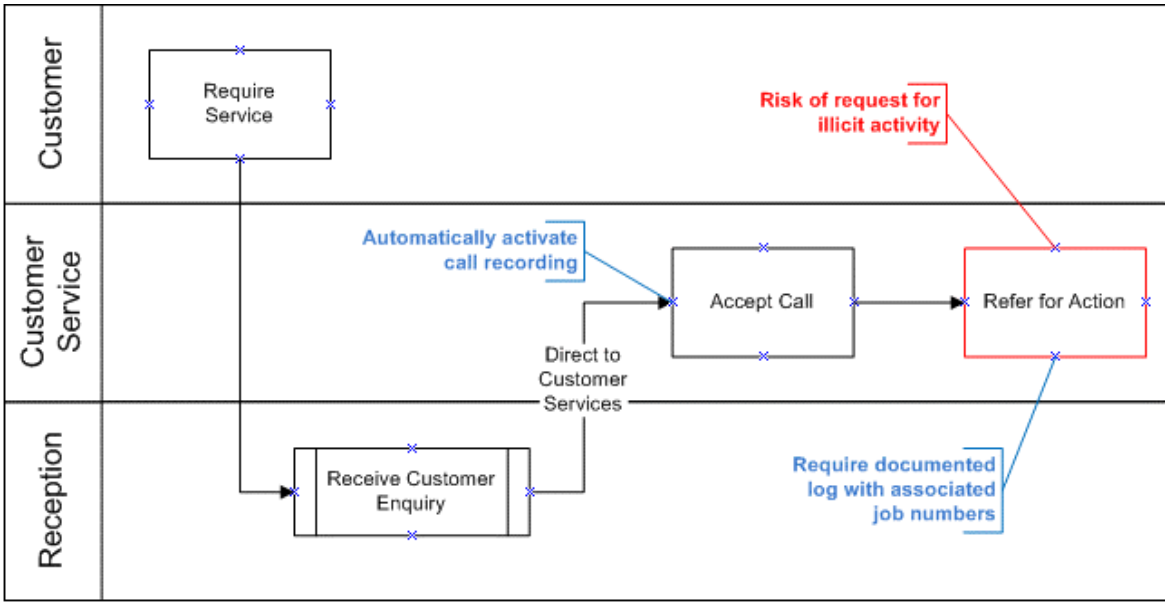


Figure 26: Processing customer communications

This is a very serious situation that should not be underestimated, especially after a more secure approach to report generation is implemented. Faced with a secure barrier to manipulating reports, attempts to subvert earlier processes, such as preparation or testing may become more likely. A 'total quality' approach to system security should not neglect this possibility.

RECOMMENDATIONS:

- Relationships between the Affiliate and its customers need to be formalised and managed in a more secure manner. In particular, the lab should have a procedure and an audit trail for any requests by clients to amend and change final test reports
- Such requests should be subject to authorisation by the Lab Manager and fully documented with date and time. Historical files of such requests should be maintained and reviewed periodically by the quality manager for any recurrent request or anomalies.
- Clients should not be able to communicate directly with testing personnel, including technicians and team leaders. All communications should be routed through a single point of contact (SPOC) and records kept for auditing.

Skills

The visit found that some aspects of organisational structure were determined by skill deficits in key personnel. Where possible, this principle should be reversed and skill shortages addressed by investment in training – particularly in 'soft skills', such as those listed above.

The Business Manager stated that although he needs to have people with technical expertise in his team, he is first looking for trust and transparency as basic qualities.

RECOMMENDATIONS:

- In addition to the essential technical skills and knowledge that are necessary for laboratory work, it is also important to ensure access to customer negotiation skills, conflict resolution and team management skills. These requirements together with strong integrity, should be part of laboratory job requirements when looking for new hires.

Staff

Systems and structures can only deliver benefits if the right personnel are in place. The Business Manager expressed his doubts about the reliability of the current service customer manager. Although he recognises that she has good technical expertise and knows the job well, she is not cooperative and she has a tendency to conceal problems with clients. He gave some examples, where the main client complained to her about an issue and she did not discuss it with him although she reports to him directly. As another example, she was asked by the Business Manager to input all pending received samples in a register (Excel worksheet), she entered all the samples except the one where there was a delay in the process entry and her manager found out later when the complaint arose from the client.

RECOMMENDATIONS:

- When recruiting laboratory employees, integrity, transparency and honesty should be emphasised as primary qualities for job applicants. Employees should be screened, tested on integrity and should have a confident personality to be able to resist clients' illicit demands.

Style

The workplace culture of the lab seems alienated from the greater whole, which is about bringing products of known quality to market. Employees perform tasks, but don't seem to understand how they contribute to achieving the mission and honouring the shared values.

There is a disconnection between what employees are doing on a daily basis at the heart of the business and the overall impact of the laboratory on quality issues and consumer products. There is a risk of disengagement. There is no Monday morning (short meeting) where managers can promote feelings of autonomy where possible by specifying results that need to be achieved and methods to achieve them and any issues that were encountered, to be solved or that have already been closed successfully.

The Business Manager specifically mentioned that when there is a problem, his team must report it to him promptly in order to find a solution together rather than having a team member burying

operational issues and finding out later when it is too late to fix it. This must be clearly communicated to all team members in order to make sure that they do not hide any information which can lead to potential problems and are not afraid to speak out.

In the case of the falsification of results by the employee who resigned. We learned that he was friends with some other members of the team who were possibly aware of his misbehaviour but remained silent because their loyalty to this employee was higher than their loyalty to the company.

RECOMMENDATIONS:

- Establish a collaborative culture by encouraging employees to report mistakes and system failures without fear. Ensure allegations about malpractice by colleagues are dealt with sensitively and with a presumption of innocence until wrongdoing is proven.

Sensemaking summary

How does something come to be a security risk event in this business?

The previous leadership had allowed an integrity problem to emerge and had failed to address it. This resulted in a series of established illicit practices and relationships within the business and with external third parties. Although previous vulnerabilities had been addressed, BPSA identified various credible displacement risks that could be exploited by a motivated offender frustrated by the hardening of the old soft spot.

What impact would it have?

The seriousness of the results adjustment, the nature of which is not disclosed in this document for reasons of confidentiality, was so severe that it could have closed the business down if not addressed in time. The displacement risks would certainly have to involve multiple employees who could be subject to bribery attempts or coercion.

What can we do about it?

The idea of running a concerted integrity management campaign was enthusiastically embraced by the new management. Staffing decisions now give integrity a much higher profile than previously and there were new recommendations about controlling external communications between individual employees and customers.

While the BPSA considered conventional security arrangements, such as building security, access control and the physical security of samples and other key tangibles, it can be seen that the greatest emphasis is on embedding security risk management and integrity into the processes themselves. In addition, the more comprehensive use of the McKinsey 7-S approach is indicative of how BPSA had matured into a more holistic approach that can welcome any specialist discipline.

CHAPTER 8: FINDINGS

In the Introduction, I wrote that my project sought to achieve three aims and I have used these as the structure for this chapter.

Quickly make sense of unfamiliar problems

- I needed a way of making sense of complex businesses and risk environments of which I had little knowledge or experience.

My project found that visualising businesses as systems provides a quick and accessible means of understanding them and that identifying and assessing risks at the process level provides an effective way of improving security and functionality – often with minimal disruption. Here, the notion of 'effectiveness' is difficult to measure in the conventional terms of reductions in the numbers of incidents or in the value of losses attributable to crime, although I hope and believe such trends may be discernible over time. What my approach does achieve is a reduction in the discernible opportunities for criminality and other intentional breaches, but it is important to recognise that this must take the form of a cyclical review, rather than a one-time fix. The problems security risk management seeks to solve are volatile and can be a product of creative and intelligent innovation by some offenders. Continuous review should not only benefit security interests, but also the wider issues of quality and efficiency. BPSA facilitates a more intimate relationship with the organisation and its activities.

The combination of methods and tools I used started to reveal a laminated view of 'risk reality'. This comprised an orderly, rational approach derived from the process-mapping, alongside a more elusive product of actors' responses to varying exposure to risk depending on their role, responsibilities and status and their respective ontologies and epistemologies.

Managers seemed more likely to be focussed on economic and performance risks, while frontline employees appeared more mindful of operational risks – particularly those likely to affect their personal well-being. These perspectives were often difficult to separate as they overlap in irregular patterns, often producing semantic fusions and occasionally revealing assumptions of common understanding when this only partly exists. A constructivist perspective suggests that the combined viewpoints of and knowledge within a group – perhaps heavily influenced by the strong views of a charismatic leadership – can also come together to form a collective view:

> Constructivist approaches regard reality as being individually and socially derived, with knowledge an individual construction that nevertheless can be subject to consensus.
>
> Costley, Elliot and Gibbs, 2010: 84

Hence, making sense of business processes must also include understanding of the cultural identities of process owners, stakeholders and other actors operating in the literal or figurative vicinity of each process. There is no quick way of doing this, so it slows the process down when the assessment is being conducted by a relative outsider. This is another reason why it is important that security risk management awareness and skills are shared with those closest to the activity.

Create a positive impact

- I needed to offer solutions that enable and enhance the business process, rather than obstruct or hinder it.

The main goal of security risk management is to change perceptions of opportunity. System managers and process owners need to develop an awareness of how their decisions can create opportunities that offenders will exploit if they identify them and find them attractive. Such decisions need to be configured to change offender perceptions and convert them from attraction to deterrence, while continuing to attract the legitimate service user or other stakeholder.

Especially in the earlier parts of my project (during which I was also 'young in service' with the company), I found that some managers were ashamed that their businesses had to engage with security function and somehow expected to be punished, while others were close to hostile because they expected a series of suffocating constraints that would impair their commercial agility. However – especially in its more developed form – BPSA really did appear to have a positive impact on allaying these fears and this was evidenced by communications expressing satisfaction to my boss, as well as feedback given to me personally.

BPSA focuses on identifying and assessing vulnerabilities and risks at the process level, then recommending solutions. Process owners who participate in BPSA either gain a new understanding or find a way of sharing existing concerns in a much more precise and structured way than with other approaches. Further, proposed solutions are discussed and negotiated with the business process in mind, rather than imposed in a 'take-it-or-leave-it' fashion.

Share the knowledge and the experience

- I needed my approach to be accessible to people with no security risk management training and to generate new knowledge to be shared with others

In terms of an approach that can be used by others, I found that managers and other employees in positions of responsibility were quick to assimilate information and even abstract ideas that they perceived to be *relevant* to their own missions and goals. This is another benefit of the process-level approach, as it involves those who own or work within each process and makes them aware of their contribution to the whole system and other systems that may lie outside their immediate space.

The application of sensemaking to the case studies – especially when done collaboratively with stakeholders – enables the extraction of learning that goes beyond the immediate circumstances of each case. I have found that it is possible to develop transferable learning to benefit other countries operating the same business and other businesses engaged in similar operational activities.

The next big challenge I have is finding an efficient means of teaching BPSA to a wider audience by remote means. Part of this challenge is how to disseminate sufficient knowledge of security and crime without requiring everyone to do a short criminology course. However, I am working on a 'primer' to incorporate in a product based on the following draft outline of 'how to do a BPSA' as part of an internal training module:

How to do a BPSA:

- Understand the setting
    - Research the country, region, city, neighbourhood, people
    - Are there any crime statistics? Does the country appear in international data pictures, such as United Nations, Transparency International and others? What does the press report? Is there any online chatter. How do people perceive the setting and how is it perceived by others?
- Understand the organisation
    - What is the leadership style? Do leaders have safety boots? (i.e. do they visit the field, or stay in the office?)
    - What is the structure and culture? Apply the 7-S
    - Who is the customer and what is the service?
    - What roles are involved in delivering the service?
    - Who would benefit from disrupting it?
    - Is there evidence of compliance or rejection of existing rules, e.g. for safety? Do people drive too fast? Do you have to sign a visitor book or show your ID?
- Map the system
    - Identify the processes and who owns them then solicit their help
    - Identify key inputs and outputs
    - Identify and evaluate existing controls, including procedures as well as any physical security implementation
    - Ask process owners about the security risks
    - Use reason and internal role-play: seek out opportunities to exploit weakness - how would you attack it?
- Recommend actions
    - Technical
    - Political/procedural
    - Organisational/cultural

To conclude this chapter, I would like to suggest that the reason a business is more secure after BPSA is because those involved have a more intimate knowledge of its working and its vulnerabilities, because of the depth of detail BPSA demands. They have been forced to understand and absorb the perceptions of others and to think about processes and their strengths and weaknesses in a different way. Security risk management is now part of their consciousness and this will hopefully affect the way they work for the better.

CHAPTER 9: CONCLUSION

My project was about developing an approach to assessing security risks that enabled a more intimate understanding of business processes, closely involving those who work within them. Having started as a way of helping me as a security practitioner learn quickly about unfamiliar businesses, it has developed into a more refined and comprehensive tool that I believe can be used effectively by managers with little or no professional security training, if they had access to specialist expertise for consultation when needed.

The report explored and discussed the core concepts as they appear in the literature and in social and commercial life. In my literature review, I located the concept of security risk management in the combined literature and perspectives of criminology, risk and management theory that provide its epistemological foundations. Criminology and the sociology of deviance provide various perspectives on offender motivation, as well as how societies and organisations formulate their own definitions of deviant behaviour. While the entire body of knowledge is useful and security practitioners should participate in and maintain an interest in its growth, the most immediately accessible concepts come from situational and opportunistic theories because these are aspects that we can influence or even control.

The discussion on risk presented the ontological debate between the natural and social sciences which I framed in the engineering, psychological and cultural perspectives. I do not accept that risk is an objective phenomenon, but I remain promiscuous as a user of these frameworks and perspectives because, as argued in the previous chapter, I believe that security risk management is about changing perceptions of risk.

I then discussed the provision of security risk management to put corporate security in an appropriate context within the literature on public and private policing. I will comment further on this in my concluding remarks below.

The chapter ended with a discussion about some of the management tools and philosophies that I find useful, including the all-important systems approach and the related concepts of quality management and the 7-S framework.

Writing in my chapter on ethics, I explained the ethics that surround my role and affirmed that my project did not require me to compromise them in any way. I explained how I had anonymised individuals, organisations and even countries to protect their respective identities. I have requested this report remain embargoed for two years, which my company confirms is acceptable. We need to balance commercial sensitivity with a desire to share our experience and participate in discussion and debate.

As the ‘research instrument’ for the project, the chapter on my positionality offered an insight into my perspective and relationship with my subject and work. I chose a biographical approach because it’s difficult to explain myself without referring to my history and life experience. What I wanted to communicate and provide evidence of is how I identify with my research subjects – including the offenders, but especially the victims. I am committed to serving them all by protecting my colleagues and influencing offenders to make better choices.

My methodology explained the research journey I have engaged with during this project and the significant transformation from an empiricist perspective that had become entrenched in my mindset, to a more pragmatic and flexible interpretivism.

This was followed by my chapter on data collection and analysis, which explained the contributions of group work, interviews, observations and role-play and the production of process maps, which were one of my most important data gathering and tools. I also used this chapter to provide a frank account of my research experience within this project and how I adapted to the challenges I encountered with the bricolage improvisations within a case study approach and sensemaking as the foundation of my analytical framework.

The four case studies were selected to illustrate how the approach developed over time from a quite narrow technique for assessing the security risks pertaining to a process or simple system, to a more comprehensive approach that is structuring a detailed analysis of complex industrial and commercial systems and hidden group dynamics. The approach remains a work in progress, but this doctoral research project has provided a solid launch platform.

> For research to be valuable from the perspective of process over product, the value must lie beyond a sense of completion. Research continues as we reflect: on the development of an idea; on data collection; on findings, and; on implications.
>
> Bourke, 2014: 1

The chapter on findings summarised the project experience in terms of what it set out to achieve and offered an outline of a training module that I am developing for non-security specialist managers.

Finally, I would like to summarise how my approach differs from other approaches and its limitations, and to discuss how it can be applied beyond the boundaries of my organisation.

First, while acknowledging and working within the context and functionality of the greater whole, my approach gathers data to identify and assess risks at a deeper, more granular level than traditional methods. Rather than *applying* security measures like paint to the exterior walls of a building, my approach integrates it *within* processes, procedures and values to project the security risk management effort into the hidden complexities of the business. In addition, the integration of security expertise with business and technical knowledge enhances the quality of preventive action by ensuring solutions are more fully aligned with business goals and performance requirements.

As most organisations are amenable to a systems approach, BPSA can be applied to the security risk management of any business, project or activity so long as it takes proper account of all relevant processes and all stakeholder perspectives. This involves collaboration with employees at all levels, not just relatively senior managers who are structurally responsible for the business or project. The voices of those who work within business processes on a routine basis have deep knowledge, but BPSA provides a framework for tapping into this and integrating it within proposed solutions.

Of course, practical constraints of time and money can limit the depth of penetration that can be achieved with limited resources. Variations in practice between different location or different businesses can impede the transferability of findings. This can be remedied by standardisation, but

this is not always appropriate as some variations are necessary adaptations to local conditions. However, these challenges are common to all approaches.

Second, my approach provides a more proactive, opportunity-oriented alternative to traditional methods of risk assessment that rely primarily on quantitative analysis of past incidents. As mentioned in my discussion of quantitative risk assessment in the Engineering Perspective section of my literature review, the reality of my organisation is that security incidents do not occur in sufficient volume to allow any meaningful quantitative analysis. However, the rare incidents that do occur have the potential to cause significant harm. While historical data is invariably useful, BPSA seeks to identify vulnerabilities that are likely to be exploited in the future. Offenders perceive these vulnerabilities as *opportunities*, so it is crucial that those seeking to protect the business find ways of empathising with the adversary and acquiring their perspective. This is the 'think criminal' component that emerges from role play and other empathic methods.

Again, all organisations have an interest in protecting themselves and preventing attacks, so this aspect of BPSA is widely applicable. However, the range of opportunities to offend appears to be expanding – particularly in the digital age. This weakens the traditional barriers of time and space and can allow offenders to attack businesses from remote locations at will. Promoting awareness of such capabilities is a major challenge that requires input to management education and access to information flows about new and emerging threats. However, BPSA and its collaborative approach can contribute to awareness-raising to encourage business actors to recognise the importance of security risk management as a core competence.

Concluding thoughts

In the 21st century the professionalisation of many security roles continues apace with the flourishing of technical and academic training programmes, a growing research and innovation culture, a proliferation of credible professional associations and an increasingly positive message about protection, quality and business enablement.

Most governments recognise that the nation state cannot sustain a monopoly on the provision of security, so the private security sector has grown exponentially in the last half century and is subject to increasing demands for quality of service and regulatory compliance.

Similar demands confront the corporate security sector, the primarily inward-facing form of security provision that is found in most organisations above a certain size and that provided the setting for this project.

Security risk management is part of the corporate security *function*, but this project proposes that it should not remain the exclusive domain of the corporate security *department*. While maintaining centralised specialist knowledge and expertise that is available to all is undoubtedly an invaluable asset, systems for disseminating the knowledge and nurturing it with feedback cycles and continuous exposure of security experts to business processes, must be put in place.

The beneficiaries of such a knowledge dissemination strategy should be those managers and other responsible post holders who are best placed to identify, assess, understand and act on the emergence of security risks in their areas of concern. I contend that they should be part of a distributed model of the security risk management function, acting with the support of centralised

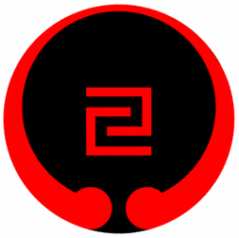
experts who can provide practical, technical and intellectual guidance to help solve the relevant problems.

This is not a manifesto for some sort of internal corporate vigilantism, as investigations and integrity management must remain in the ownership of specialists who are trusted and known to act only in the interests of the company – which must *always* be defined in terms of compliance to legal, ethical and accepted moral norms. Rather, it proposes a programme of empowerment and opportunity to ensure the quality, integrity and sustainability of business processes and the organisation's functional capability.

It would be helpful to see security risk management appear as a core subject on MBA and similar mainstream management programmes. Its omission makes no sense, while its inclusion would bring many benefits – including providing students with the means of interpreting security risk situations and advice within a recognised and proven framework.

However, in the meantime, I will continue to immerse myself in my organisation's businesses, systems, processes and people to learn from them and to evangelise by all available means.

As I reflect on the multi-disciplinarity of my subject matter and its lack of homogeneity, I am conscious of its irregular fit – when taken as an amorphous whole – with any of the disciplines that contribute to it. Without the practical experience of using this approach in business – and the invaluable feedback and endorsement by my organisation, I would fear that all my talk of 'changing perceptions' and 'opportunity reduction' would attract accusations of peddling snake-oil. However, I think the systems approach provides an invaluable bridge between hard and soft aspects of people, organisations and the world.



This symbol 'expresses the harmony of hardness and softness in nature' (IOGKF, 2011), characterising heaven as round, softly embracing and protecting a hard earth. It is the badge of *Gōjū-ryū* (剛柔流), the original 'hard-soft' style of karate from the island of Okinawa and the first martial art I practiced. The philosophies associated with it continue to have a lasting influence on my life and career.

REFERENCES

AAAS-FBI-UNICRI (2014) *Risk assessment framework*. Washington DC: AAAS.

Adams, J. (2000) *Risk*. London: UCL Press.

AIRMIC, ALARM and IRM (2010) *A structured approach to enterprise risk management (ERM) and the requirements of ISO 31000* https://www.theirm.org/media/886062/ISO3100_doc.pdf [accessed 12 May 2018].

Akers, R.L., Krohn, M.D., Lanza-Kaduce, L. and Radosevich, M. (1979) 'Social learning and deviant behavior: A specific test of a general theory'. *American Sociological Review* 44 (4): pp 636-655.

Anderson, D.A. (2002) 'The deterrence hypothesis and picking pockets at the pickpocket's hanging'. *American Law and Economics Review* 4 (2): pp 295-313.

Andrews, N. (2008) *The modern civil process: Judicial and alternative forms of dispute resolution in England*. Tubingen: Mohr Siebeck.

Anonymous (2005) 'A world of difference: Ex-cops are popular recruiting targets for top security job but that background can be bad for business'. *CSO: The resource for security executives* July pp 52-53.

Aoki, M. (1986) 'Horizontal vs. vertical information structure of the firm'. *The American Economic Review* 76 (5): pp 971-983.

Appelbaum, S. (1997) 'Socio-technical systems theory: an intervention strategy for organizational development'. *Management Decision* 35 (6): pp 452-463.

Arbnor, I. and Bjerke, B. (2009) *Methodology for creating business knowledge*. London: Sage.

ASIS International (2003) *The General Security Risk Assessment Guideline*. Alexandria, Virginia: ASIS International.

Aspers, P. (2004) *Empirical phenomenology: An approach for qualitative research*, Papers in Social Research Methods, Qualitative Series No 9, London School of Economics and Political Science Methodology Institute.

Bamfield, J. (2014) 'Security purpose: an ever-expanding remit' in Gill, M. (Ed) (2014) *The Handbook of Security* Basingstoke: Palgrave-Macmillan.

Beccaria, C. (1764) *An essay on crimes and punishments*, *2nd American Edition.* (1819), Philadelphia: Nicklin.

Beck, A. and Willis, A. (1995) *Crime and security: managing the risk to safe shopping*. Leicester: Perpetuity Press.

Beck, U. (1992) *Risk society: Towards a new modernity*. (Translated from the original 1986 German by Mark Ritter) London: Sage.

Bennett, T. and Wright, R. (1984) *Burglars on burglary: prevention and the offender.* Aldershot: Gower.

Bentham, J. (1781) *An introduction to the principles of morals and legislation*, *2000 Edition*. Kitchener ON: Batoche Books.

Bentham, J. (1894) *Theory of legislation*. (trans. Dumont, E) London: Trubner.

Berlinger, R.B. (2000) *Introduction to research methods.* London: Sage.

Bertalanffy, L. von, (1934) *Modern theories of development.* (Translated by JH Woodger) Oxford: Oxford University Press.

Bertalanffy, L. von (1972) 'The history and status of general systems theory'. *The Academy of Management Journal* 15 (4): pp 407-426.

Borrion, H (2013) 'Quality assurance in crime scripting'. *Crime science: An interdisciplinary journal* 2: 6 https://doi.org/10.1186/2193-7680-2-6 [Accessed 29 June 2018]

Bourke, B. (2014) 'Positionality: Reflecting on the research process'. *The Qualitative Report* 19: How to article 18: pp 1-9.

Brantingham, P.J. and Brantingham, P.L. (1991) 'Introduction: The dimensions of crime'. in Brantingham, P.J. and Brantingham, P.L. (Eds.) *Environmental Criminology, 2nd edition.* Prospect Heights, IL: Waveland Press.

Briggs, R. and Edwards, C. (2006) *The business of resilience: Corporate security for the 21st century.* London: Demos.

British Retail Crime Survey (2013) cited on http://www.kingdom.co.uk/articles/effect-of-retail-crime-on-businesses.aspx [accessed 21 June 2015].

Brooks, D.J. and Corkhill, J. (2014) 'Corporate security and the stratum of security management' in Walby, K. (Ed) *Corporate security in the 21st century.* London: Palgrave Macmillan.

Brown, A.D., Colville, I. and Pye, A. (2015) 'Making sense of sensemaking in organization studies'. *Organization Studies* 36 (2): pp 265-277.

Burns, R.B. (2000) *Introduction to research methods.* London: Sage.

Button, M. and George, B. (1995) 'Why some organisations prefer contract to in-house security staff' in Gill, M. (Ed) *Crime at work: Increasing the risk for offenders.* Leicester: Perpetuity Press.

Button, M. (2016) *Security officers and policing: Powers, culture and control in the governance of private space.* Oxford: Routledge.

Campbell Institute (2014) *Risk perception: Theories, strategies, and next steps*, National Safety Council http://www.nsc.org/CambpellInstituteandAwardDocuments/WP-Risk%20Perception.pdf [accessed 02 January 2017].

Center for Strategic and International Studies (2013) *The economic impact of cybercrime and cyber espionage* http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime.pdf [accessed 10 June 2015].

Chartered Quality Institute (2015) 'What is quality?' http://www.thecqi.org/The-CQI/What-is-quality/ [accessed 25 June 2015].

Christopher, K. (2015) *Port Security Management*, *2nd Edition*. Boca Raton, USA: CRC Press.

Clarke, R.V. (Ed) (1997) *Situational crime prevention: Successful case studies, 2nd Edition*. Albany, NY: Harrow and Heston.

Cloward, R.A. and Ohlin, L.E. (1960) *Delinquency and opportunity: A study of delinquent Gangs.* New York: The Free Press.

Coetzee, B. & Horn, R. (2006) *The Theft of Precious Metals from South African Mines and Refineries*. Pretoria, RSA: Institute for Security Studies.

Coghlan, D. and Brannick, T. (2014) *Doing action research in your own organization*, *4th Edition.* London: Sage.

Cohen, A.V. (1996) 'Quantitative risk assessment and decisions about risk: an essential input into the decision process' in Hood, C. and Jones, D. (Eds) (1996) *Accident and design: contemporary debates in risk management.* London: UCL Press.

Cohen, L.E. & Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach'. *American Sociological Review* 44: 588-608.

Cooper, J.A. (2015) *Twentieth-century influences on twenty-first-century policing: Continued lessons of police reform.* London: Lexington Books.

Cornish, D.B. and Clarke, R.V. (2003) 'Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention'. *Crime Prevention Studies* 16: 41-96.

Costley, C., Elliott, G.C. and Gibbs, P. (2010) *Doing work based research: Approaches to enquiry for insider-researchers.* London: Sage.

Crosby, P. (1984) *Quality without tears*. New York: McGraw-Hill (1995 Edition).

D'aveni, R.A. (1994) *Hypercompetition.* New York: The Free Press.

Dalton, D.R. (2003) *Rethinking corporate security in the post-9/11 era: Issues and strategies.* USA: Elsevier.

DeLisi, M. (2012) 'Genetics: L'enfant terrible of criminology'. *Journal of Criminal Justice* 40: 515-516.

Dempsey, J. (2008) *Introduction to private security law.* Belmont, CA: Thompson Higher Education.

Ditton, J. (1977) *Part-time crime: An ethnography of fiddling and pilferage.* London: MacMillan.

Douglas, M. and Wildavsky, A. (1982) *Risk and culture.* Los Angeles: University of California Press.

Douglas, M. (2006) *A history of grid and group cultural theory.* Semiotics Institute Online http://projects.chass.utoronto.ca/semiotics/cyber/douglas1.pdf [accessed 03 May 2017].

Downes, D. and Rock, P. (1995) *Understanding deviance: A guide to the sociology of crime and rule-breaking*, *Revised 2nd Edition.* Clarendon Press: Oxford.

Dul, J. and Hak, T. (2008) *Case study methodology in business research.* London: Elsevier.

Duymedjian, R. and Rüling, C. (2010) 'Towards a foundation of bricolage in organization and management theory'. *Organization Studies* 31 (2): pp 133-151.

England, K. V. L. (1994) 'Getting personal: Reflexivity, positionality, and feminist research'. *The Professional Geographer*, 46: 80-89.

Fayol, H. (1916) *Administration Industrielle Et Générale.* http://mip-ms.cnam.fr/servlet/com.univ.collaboratif.utils.LectureFichiergw?ID_FICHIER=1295877017978 [accessed 07 April 2015].

Feilzer, M.Y. (2010) 'Doing mixed methods research pragmatically: Implications of the rediscovery of pragmatism as a research paradigm'. *Journal of Mixed Methods Research* 4 (1): pp 6-16.

Felson, M. and Clarke, R.V. (1998) *Opportunity makes the thief: Practical theory for crime prevention.* Police Research Series Paper 98, London: Home Office Policing and Reducing Crime Unit.

Gabor, A. and Mahoney, J.T. (2010) 'Chester Barnard and the systems approach to nurturing organizations' University of Illinois College of Business Working Papers https://business.illinois.edu/working_papers/papers/10-0102.pdf [accessed 19 April 2016].

Garland, D. (1997) 'Of crimes and criminals: The development of criminology in Britain' in Maguire, M., Morgan, R. and Reiner, R. (1997) *The Oxford Handbook of Criminology – Second Edition.* Oxford: Clarendon Press.

Garland, D. (2001) *The culture of control.* Oxford: Oxford University Press.

George, B. and Button, M. (1994) 'Why some organisations prefer in-house to contract security staff' in Gill, M. (Ed) *Crime at work: Studies in security.* Leicester: Perpetuity Press.

Giddens, A. (1999) 'Risk and responsibility'. *Modern Law Review* 62: 1-10.

Gigerenzer, G. (2008) 'Why heuristics work'. *Perspectives on Psychological Science* 3 (1): pp 20-29.

Gill, M. (2000) *Commercial robbery: Offenders' perspectives on security and crime prevention*. London: Blackstone Press.

Gill, M. (Ed.) (1998) *Crime at work: Increasing the risk for offenders 2*. Leicester: Perpetuity Press.

Gill, M. (Ed) (2014) *The handbook of security.* Basingstoke: Palgrave.

Gill, M. and Hart, J. (1996) 'Historical perspectives on private investigation in Britain & the US'. *Security Journal* 7: pp 273-280.

Gill, M. and Hart, J. (1997) 'Exploring Investigative Policing: Private Detectives in Britain'. *British Journal of Criminology* 37: pp 549-567.

Gill, M. and Hart, J. (1997b) 'Private investigators in Britain & America'. *Policing: An International Journal of Police Strategies and Management* 20 (4): pp 631-640.

Gill, M. and Hart, J. (1997c) 'Policing as a business: The organisation and structure of private investigation'. *Policing and Society* 7 (2): pp 117-141.

Gill, M. and Hart, J. (1999) 'Enforcing corporate security policy using private investigators'. *European Journal on Criminal Policy and Research* 7 (2): pp 245-261.

Gill, M. and Hart, J. (1999) 'Investigative policing in Britain: the public-private divide' in Ocqueteau, F (Ed.) *Police et Securité: contrôle social et interaction public/privé.* Paris, France: GERN pp 169-178.

Gill, M., Hart, J. and Livingstone, K. (2000) 'Evaluating the crime desk & its role as investigator'. *Policing: An International Journal of Police Strategies and Management* 23 (2): pp 246-259.

Gill, M., Hart, J. and Stevens, J. (1996) 'Private investigators: Under-researched, under-estimated and under-used?'. *International Journal of Risk, Security and Crime Prevention* 1 (4): pp 305-313.

Gill, M., Hart, J., Livingstone, K. and Stevens, J. (1996) *The crime allocation system: Police investigations into burglary and auto crime*. London: Home Office.

Gillham, B. (2010) *Case study research methods.* London: Bloomsbury Publishing PLC.

Gray, E., Jackson, J. and Farrell, S. (2008) 'Reassessing the fear of crime'. *European Journal of Criminology* 5 (3): pp 363-380.

Haelterman, H (2016) *Crime script analysis: Preventing crimes against business.* London: Springer.

Haimes, Y.Y. (2015) *Risk modelling, assessment, and management*. London: John Wiley and Sons.

Hammersley, M. and Atkinson, P. (2007) *Ethnography: Principles in practice*. Abingdon: Routledge

Harland, T. (2014) 'Learning about case study methodology to research higher education'. *Higher Education Research and Development* 33 (6): pp 1113-1122.

Harrison, H., Birks, M., Franklin, R. and Mills, J. (2017) 'Case study research: Foundations and methodological orientations'. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 18 (1) Art 19
http://nbn-resolving.de/urn:nbn:de:0114-fqs1701195
[accessed 01 December 2017].

Hart, J. (1993) *Total quality security: Quality management and corporate security*, unpublished dissertation, submitted as part-fulfilment of the Master of Science in Security Management and Information Technology, Centre for the Study of Public Order, University of Leicester.

Hart, J. (2004) 'Shoplifters on shoplifting'. *British Retail Consortium Yearbook 2004* London: The Stationery Office.

Hart, J. (2010) 'Criminal infiltration of financial institutions: a penetration test case study'. *Journal of Money Laundering Control* 13 (1): pp 55-65.

Hart, J. and Evans, G. (2012) 'Border Security & DocEx: controlling the manipulation of identity' conference presentation. *SMI Border Security* Sofia, Bulgaria.

Henry, S. (2015) *Private justice: Towards integrated theorising in the sociology of law*. New York: Routledge.

Holt, R. and Cornelissen, J. (2014) 'Sensemaking revisited'. *Management Learning*. 45 (5): pp 525-539.

Hood, C. and Jones, D. (Eds.) (1996) *Accident and design: contemporary debates in risk management.* London: UCL Press.

Hoogenboom, B. (1991) 'Grey policing: A theoretical framework'. *Policing and Society* 2 (1): pp 17-30.

Hooton, E.A. (1939) The American criminal. Cambridge: Harvard University Press.

Institute of Risk Management (2002) *A risk management standard*. London: IRM.

Institute of Risk Management (2018) *A risk practitioner's guide to ISO 31000:2018*. London: IRM.

International Organization for Standardization (2018). *Risk management: ISO31000*
https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf
[Accessed 05 May 2018]

Jeffrey, C.R. (1971) *Crime prevention through environmental design*. Beverley Hills, CA: Sage.

Jeffrey, C.R. and Zahm, D.L. (1993) 'Crime prevention through environmental design, Opportunity theory and rational choice models' in Clarke, R.V. and Felson, M. (Eds.) (1993) *Routine activity and rational choice: Advances in criminological theory volume 5.* New Brunswick: Transaction Publishers.

Johnston, L. (1992) *The rebirth of private policing*. London: Routledge.

Johnstone, V., Leitner, M., Shapland, J. and Wiles, P. (1994) *Crimes and other problems on industrial estates*. Crime Prevention Unit Paper 54 London: Home Office.

Khanyile, D. and Cluett, J. (2017) 'Sensemaking and unknowable in risk management'. ResearchGate https://www.researchgate.net/publication/317370650_SENSEMAKING_AND_UNKNOWABLE_IN_RISK_MANAGEMENT [accessed 03 February 2018].

Kathawala, Y. (1989) 'A comparative analysis of selected approaches to quality'. *International Journal of Quality & Reliability Management* 6 (5): 7-17.

Kincheloe, J. (2004) 'Introduction: the power of the bricolage: expanding research methods' in Kincheloe, J. and Berry, K. (2004) *Rigour and complexity in educational research: Conceptualizing the bricolage.* London: Open University Press.

Kletz, T.A. (1999) 'The origins and history of loss prevention'. *Process Safety and Environmental Protection* 77 (3): pp 109-116.

Knight, F. (1921) *Risk, uncertainly and profit.* (1964 reprint) New York: Kelley.

Knoema Corporation (2015) *World Data Atlas.* https://knoema.com/atlas [accessed 04 April 2015].

Koontz, H. (1961) 'The management theory jungle'. *Journal of the Academy of Management* 4 (3): pp 174-189.

Lalonde, C. and Boiral, L. (2012) 'Managing risks through ISO 31000: a critical analysis'. *Risk Management*, 14: 272-300.

Lark, J. (2015) *ISO3100 Risk management: A practical guide for SMEs.* Geneva: International Standards Organisation.

Layder, D. (1993) *New strategies in social research*. Cambridge, MA: Polity Press.

Leitch, M. (2010) 'The fundamental flaws in ISO's definition of 'risk' http://www.workinginuncertainty.co.uk/isoriskdefinition.shtml [accessed 09 March 2016].

Lichtenstein, S., Slovic, P., Fischoff, B., Layman, M. and Combs, B. (1978) 'Judged frequency of lethal events'. *Journal of Experimental Psychology: Human Learning and Memory* 4: 6 November.

Lippert, R., Walby, K. and Steckle, R. (2013) 'Multiplicities of corporate security: Identifying emerging types, trends and issues'. *Security Journal* 26 (3): pp 206-221.

Livingstone, K. and Hart, J. (2003) 'The wrong arm of the law: popular representations of private security'. *Policing and Society* 13: 159-170.

Lombroso, C. (1878) *L'Uomo delinquente, 2006 Edition*, edited by Gibson, M. and Rafter, N.H., London: Duke University Press.

Manunta, G. (1998) *Security: An introduction.* Shrivenham: Cranfield University Press.

Mars, G. (1984) *Cheats at work: An anthropology of work place crime.* London: Allen and Unwin.

Maslow, A.H. (1943) 'A theory of human motivation'. *Psychological Review* 50 (4): pp 370-96.

Mastercard (2013) 'MasterCard Study Reveals the Rapidly Growing Cashless Economies'. http://newsroom.mastercard.com/press-releases/mastercard-study-reveals-the-rapidly-growing-cashless-economies/ [accessed 03 April 2015].

Meerts, C. and Dorn, N. (2009) 'Corporate security and private justice: Danger signs?' *European Journal of Crime, Criminal Law and Criminal Justice* 17: 97-111.

Merton, R.K. (1938) 'Social structure and anomie'. *American Sociological Review* 3 (5): pp 672–682.

Microsoft Corporation (2009) *Microsoft Application Architecture Guide, 2nd Edition*. https://msdn.microsoft.com/en-us/library/ff650706.aspx [accessed 03 February 2018].

NaCTSO (2015) *Guidance: Industry preparedness.* https://www.gov.uk/government/publications/industry-preparedness/industry-preparedness [accessed 02 December 2017].

Narayan, D., Chambers, R., Shah, M.K. and Petesch, P. (2000) *Voices of the poor: Crying out for change.* Washington DC: The World Bank.

Newman, O. (1972) *Defensible space: People and design in the violent city.* New York: Macmillan

Okinawan Traditional Goju Ryu Karate-do Association (2011) 'Explanation of the IOGKF Badge' http://www.otgka.co.uk/explanation-of-the-iogkf-badge.html [Accessed 01 March 2018]

O'Sullivan, C. (2018) 'Role-play and research' in Cohen, L., Manion, L. and Morrison, K (Eds.) *Research Methods in Education*, New York: Routledge

Oxford English Dictionary (2017) https://en.oxforddictionaries.com/definition/security [accessed 02 January 2017].

Overseas Security Advice Council (OSAC), US Department of State Bureau of Diplomatic Security https://www.osac.gov/pages/Home.aspx [accessed 03 April 2015].

Paget, M.A. (1988) *The unity of mistakes: A phenomenological interpretation of medical work*. Philadelphia: Temple University Press.

Parkhe, A. (1993) 'Messy research, methodological predispositions, and theory development in international joint ventures'. *Academy of Management Review* 18 (2): pp 227-268.

Petersen, K.L. (2014) 'The politics of corporate security and the translation of national security'. in Walby, K. (Ed) *Corporate security in the 21st century.* London: Palgrave Macmillan.

Pfadenhauer, M. and Grenz, T. (2015) 'Uncovering the essence: The why and how of supplementing observation with participation in phenomenology-based ethnography'. *Journal of Contemporary Ethnography* 44 (5): pp 598-616.

Pietersma, H. (2000) *Phenomenological epistemology*. New York: Oxford University Press.

Polanyi, M. (1966) *The tacit dimension.* Chicago: University of Chicago Press.

Provost, C. (2017) 'The industry of inequality: why the world is obsessed with private security'. *The Guardian,* 12 May https://www.theguardian.com/inequality/2017/may/12/industry-of-inequality-why-world-is-obsessed-with-private-security [accessed 12 November 2017].

Purpura, P. (2013) *Security and loss prevention: An introduction, 6th Edition.* Oxford: Elsevier.

Reiner, R. (2000) *The politics of the police, 3rd Edition*. Oxford: Oxford University Press.

RHQ RMP (2018) *The Royal Military Police Museum* https://www.rhqrmp.org/rmp_museum.html [accessed 08 February 2018].

Rogers, K. (2016) 'A brief history of loss prevention'. *Loss Prevention Insider* http://losspreventionmedia.com/insider/loss-prevention/a-brief-history-of-loss-prevention/ [accessed 12 December 2017].

Rogers, M. (2012) 'Contextualizing theories and practices of bricolage research'. *The Qualitative Report* 17 (7): pp 1-17.

Ropohl, G. (1999) 'Philosophy of socio-technical systems'. *Techné: Research in philosophy and technology* 4 (3): pp 186-194.

Rovers, J. (2014) 'Security is always too much when nothing happens and never enough when an incident occurs'

http://www.afimacglobal.com/jrovers/2014/09/26/security-is-always-too-much-when-nothing-happens-and-never-enough-when-an-incident-occurs/
[accessed 07 Sep 2017].

Schwarz, M. and Thompson, M. (1990) *Divided we stand: Redefining politics, technology and social choice.* Philadelphia: University of Pennsylvania Press.

Seligman, D. (1957) 'The enduring slums' in Whyte, W.H. Jr (Ed.) (1957) *The exploding metropolis.* New York: Doubleday.

Shaw, C.R. and McKay, H.D. (1942) *Juvenile delinquency in urban areas.* Chicago: University of Chicago Press.

Shearing, C.D. and Stenning, P.C. (1979) 'Private security and private justice'. *British Journal of Law and Society* 6 (2): pp 261-271.

Shearing, C.D. and Stenning, P.C. (1983) 'Private security: Implications for social control'. *Social Problems* 30 (5): pp 493-506.

Shearing, C.D. and Stenning, P.C. (1983) *Private security and private justice: The challenge of the 80s.* Quebec: Institute for Research on Public Policy.

Simon, H.A. and Newell, A. (1958) 'Heuristic problem solving: the next advance in operations research'. *Operations Research* January-February, 1-10.

Simon, H.A. (1956) 'Rational choice and the structure of the environment'. *Psychological Review* 63 (2): pp 129-138.

Singer, J.D. (1958) 'Threat-perception and the armament-tension dilemma'. *The Journal of Conflict Resolution* 2 (1): pp 90-105.

Skyttner, L. (2005) *General systems theory: Problems, perspectives, practice*. Singapore: World Scientific Publishing.

Speight, P. (2012) *Why security fails: How the academic view of security can be balanced with the realities of operational delivery.* Ossett, W Yorks: Protection Publications.

Stephenson, S. (2017) 'It takes two to tango: The state and organized crime in Russia'. *Current Sociology* 65 (3): 411-426.

Sutherland, E.H. (1949) *White collar crime.* New York: Dryden Press.

Talbot, J. and Jakeman, M. (2009) *Security risk management body of knowledge*. New Jersey: Wiley.

Taylor, I.R., Walton, P. and Young, J. (2013) *The new criminology: for a social theory of deviance* (40th Anniversary Edition). London: Routledge.

Transparency International (2014) *Corruption Perceptions Index 2014*
https://www.transparency.org/news/feature/corruption_perceptions_index_2014
[accessed 04 April 2015].

Travis, L.F. and Edwards, B.D. (2015) *Introduction to criminal justice.* 8th Edition, Waltham MA: Elsevier.

Trist, E. (1981) 'The evolution of socio-technical systems: a conceptual framework and an action research program., *Occasional Paper No 2: June*. Toronto: Ontario Ministry of Labour.

Tsang, E.W.K. (2013) 'Case study methodology: causal explanation, contextualization, and theorizing'. *Journal of International Management* 19: 195-202.

United Nations (1945) *United Nations Charter*
http://www.un.org/en/charter-united-nations/index.html
[accessed 08 May 2016].

Van Oppen, C. (2002) 'The role of insurance in disaster reduction'. *Journal of Business Perspective* July-December: 1-10.

Vellani, K. (2006) *Strategic security management: A risk assessment guide for decision makers.* Oxford: Elsevier.

Vold, G.B. and Bernard, T.J. (1986) *Theoretical criminology.* New York: Oxford University Press.

Waddington, P.A.J. (1999) *Policing citizens: Authority and rights.* London: UCL Press.

Wakefield, A. and Button, M. (2014) 'Private policing in public spaces' in Reisig, M.D. and Kane, R.J. (Eds.) *The Oxford Handbook of Police and Policing.* Oxford: Oxford University Press.

Wakefield, A. (2000) 'Situational crime prevention in mass private property*'* in Hirsch, A., Garland, D. and Wakefield, A. (Eds.) *Ethical and social perspectives on situational crime prevention*. Portland, USA: Hart Publishing.

Wakefield, A. (2014) 'Corporate security and enterprise risk management'. in Walby, K. and Lippert, R.K. (Eds.) (2014) *Corporate security in the 21st century*. London: Palgrave Macmillan.

Walby, K. Luscombe, A. and Lippert, R.K. (2014) 'Expertise and the professionalization of municipal corporate security in Canadian cities' in Walby, K. (Ed.) *Corporate security in the 21st century.* London: Palgrave Macmillan.

Walby, K. and Lippert, R.K. (2014) 'Governing every person, place and thing – critical studies of corporate security' in Walby, K. (Ed) *Corporate security in the 21st century.* London: Palgrave Macmillan.

Waterman, R., Peters, T.J. and Phillips, J.R. (1980) 'Structure is not organization'. *Business Horizons* 23 (3): pp 14-26.

Weick, K.E., Sutcliffe, K.M. and Obstfeld, D. (2006) 'Organizing and the process of sensemaking'. *Organization Science* 16 (4): pp 409-421.

Williams, J.W. (2014) 'The private eyes of corporate culture: The forensic accounting and corporate investigation industry and the production of corporate financial security' in Walby, K. and Lippert, R.K. (Eds) (2014) *Corporate security in the 21st century.* London: Palgrave Macmillan.

Williams, L. (Ed) (2016) *Crime against businesses: findings from the 2015 Commercial Victimisation Survey.* London: Home Office.

Wilson, J.Q. and Kelling, G.L. (1982) 'Broken windows: the police and neighborhood safety'. *Atlantic Monthly* 249 (3): pp 29–38.

Wilson, J.Q. (1983) *Thinking about crime (revised edition)*. New York: Basic Books.

Woodside, A.G. and Wilson, E.J. (2003) 'Case study research methods for theory building'. *Journal of Business and Industrial Marketing* 18 (6/7): pp 493-508.

Yin, R.K. (2009) *Case study research: design and methods*. London: Sage.

Znaniecki, F. (1940) *The social role of the man of knowledge.* New York: Columbia University Press.